

HIPAA 101: Facing Your Fears & Balancing the Needs



HIPAA Training For DMH Providers
Harry S. Truman Office Building
September 4 - 5, 2002



Disclaimer

(For Non-DMH Personnel)



- ▶ The Missouri Department of Mental Health does not give legal advice, nor allege any legal expertise. Information and advice provided should be accepted as general in nature to guide the Missouri Department of Mental Health and its facilities' HIPAA Core Teams. Any and all other parties should consult professional counsel for specific legal advice.
- ▶ The information contained herein or otherwise presented in any format is compiled from official sources within and outside the Missouri Department of Mental Health. The use of the enclosed materials is approved for compliance activities and other official business only, and is in no way intended to assert any guarantee of HIPAA Compliance.
- ▶ Beyond the use as an educational resource only, any and all other use of the material is strictly prohibited. Any misappropriation or misuse of the materials should be reported immediately to Ann Dirks-Linhorst, Missouri Department of Mental Health Interim Privacy Officer

HIPAA Overview:

Digging through the muck



Janet Conboy
HIPAA Project Coordinator
Missouri Department of Mental Health

Health Insurance Portability and Accountability Act of 1996

- ▶ Federal Law (Public Law 104-191)
 - ▶ Don't shoot the messenger
- ▶ Purpose
 - ▶ Addresses group health plan requirements
 - ▶ Expands fraud and abuse enforcement abilities
 - ▶ Provides for health insurance portability
 - ▶ Promotes medical savings accounts
 - ▶ Establishes **Administrative Simplification Standards**

HIPAA Titles

- ▶ Title I: Portability of health insurance
- ▶ Title II: Preventing healthcare fraud and abuse
 - ▶ **Administrative simplification (subtitle F)**
- ▶ Title III: Tax related provisions - medical savings accounts
- ▶ Title IV: Group health plan requirements
- ▶ Title V: Revenue offsets

Impact

- ▶ Called the most sweeping legislation to affect the health care industry in more than 30 years
- ▶ Will affect almost all healthcare transaction processes as well as systems that generate or store data
- ▶ Most experts agree cost of compliance will outdistance Y2K (AHA estimates \$22.5 billion over 5 years)
- ▶ Regulations (except privacy) supercede state laws, unless the secretary grants the state a waiver.
 - ▶ Privacy rule supercedes only those portions of other federal or state law or regulation that provide less protection

Administrative Simplification

- ▶ Covered Entities must comply
 - ▶ Health Plans
 - ▶ Healthcare Clearing Houses
 - ▶ Healthcare Providers who conduct any of the covered transactions electronically
- ▶ Definition of Electronically includes
 - ▶ Transmission by Internet, Intranets, leased lines, dial-up lines, private networks
 - ▶ Physical movement of data on diskette, CD, magnetic tape, etc.
- ▶ Covered Entities must pass many responsibilities to Business Associates
 - ▶ Anyone who receives PHI as part of doing business for the Covered Entity

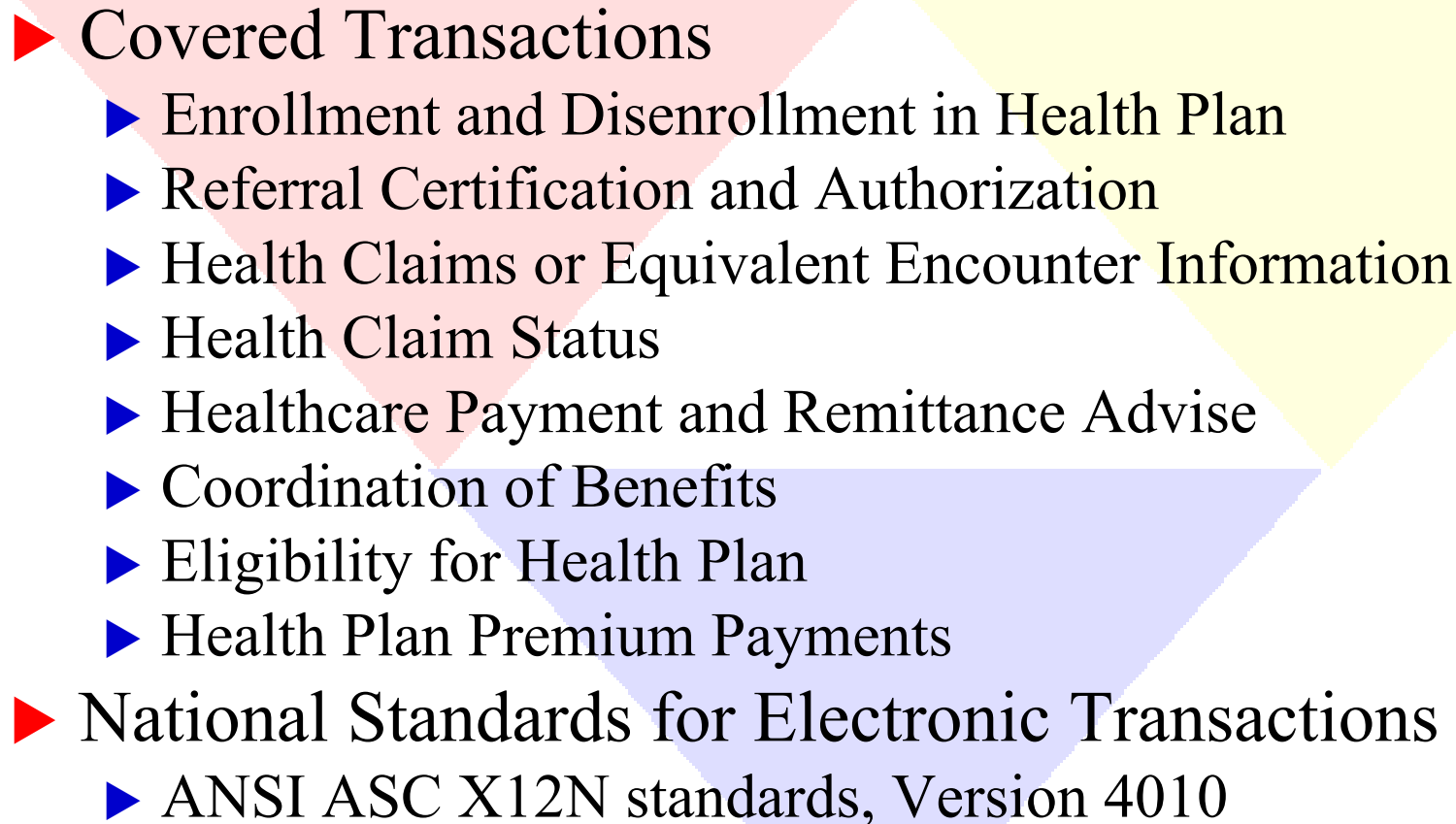
Administrative Simplification

- ▶ Establishes and requires national standards for:
 - ▶ Electronic transactions
 - ▶ Transaction sets - claims related transactions (Oct. 02 or 03)
 - ▶ Code sets: diagnosis, therapeutic, & treatment (Oct. 02)
 - ▶ Identifiers: provider, payer (Pending), individual (On Hold)
 - ▶ Privacy/confidentiality (April 03)
 - ▶ To protect protected healthcare information (PHI) from misuse
 - ▶ Security (Proposed)
 - ▶ Safeguards around client information systems preventing unauthorized access
- ▶ Designated Standard Maintenance Organizations
 - ▶ All standards must be established by these organizations

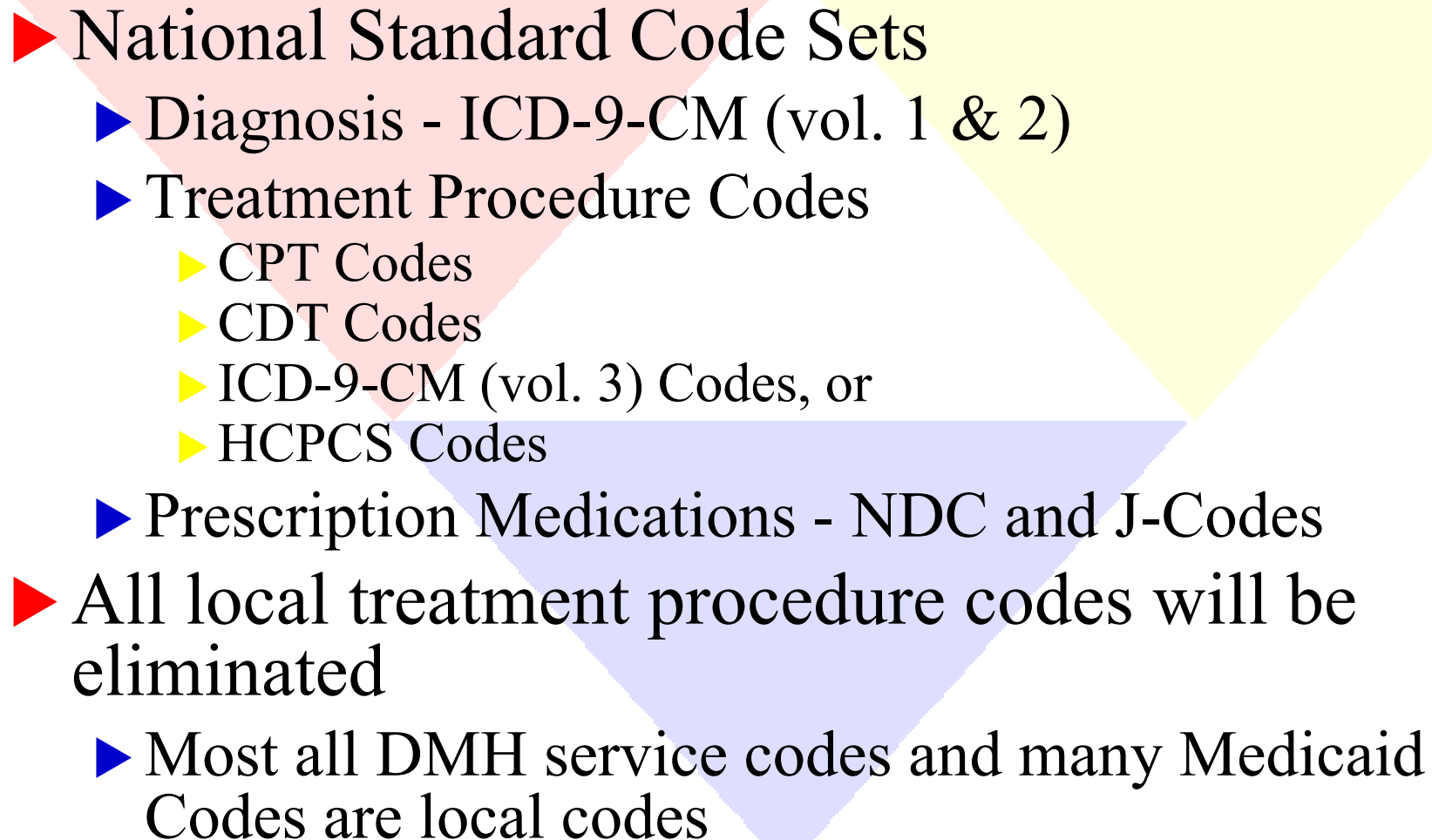
Status of Regulations

<i>Standard</i>	<i>Proposed Rule Publication Date</i>	<i>Final Rule Effective Date</i>	<i>Compliance Date</i>
Transactions & Code Sets	May 7, 1998	October 2000	October 2002 or 2003
Privacy	November 3, 1999	April 2001	April 2003
Security	August 12, 1998		Two years after final
Individual Identifier	On hold	On hold	On hold
Employer Identifier	June 16, 1998	May 2002	Two years after final
Provider Identifier	May 7, 1998		Two years after final

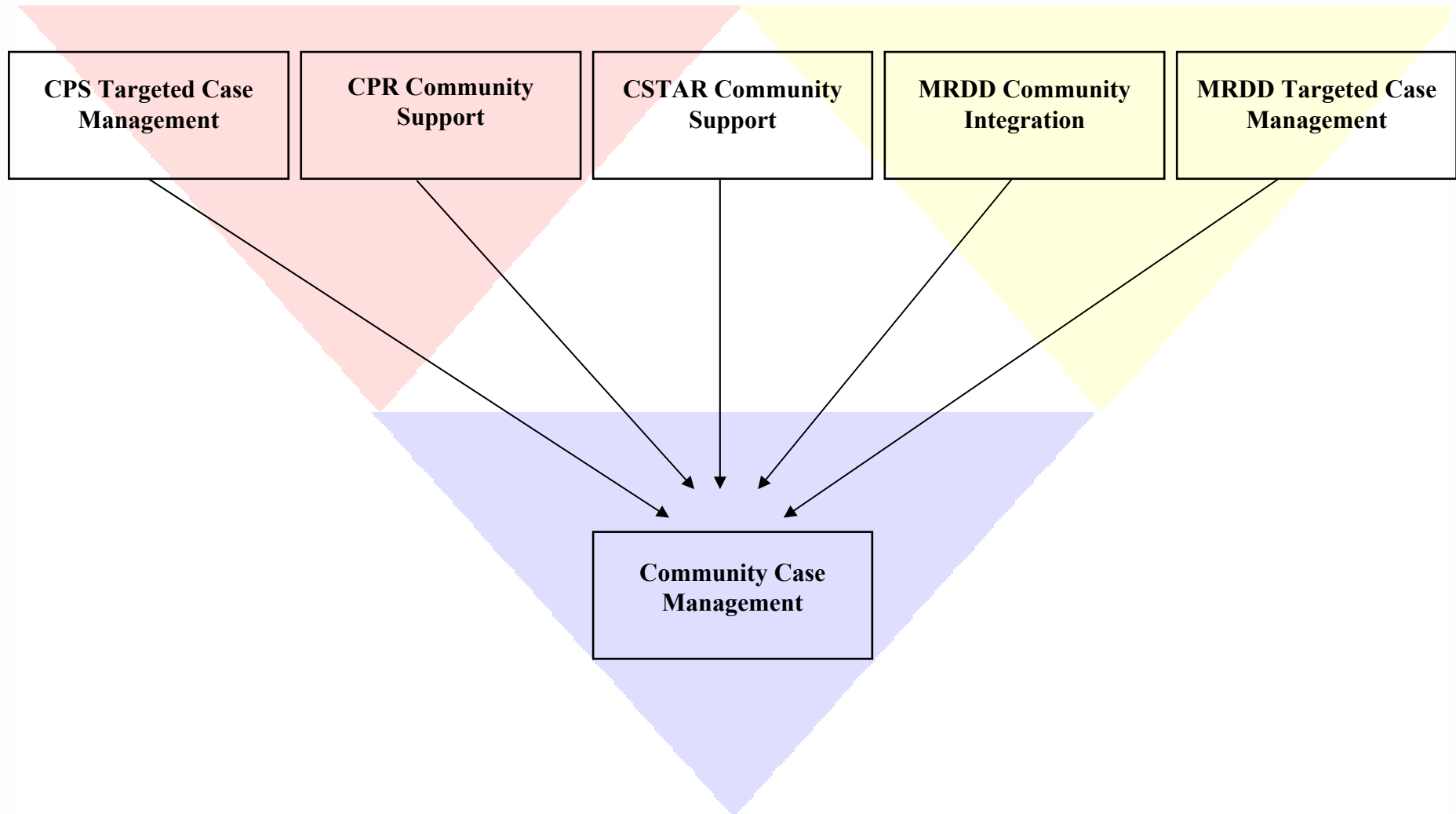
Transactions (Oct. 2002)

- 
- ▶ Covered Transactions
 - ▶ Enrollment and Disenrollment in Health Plan
 - ▶ Referral Certification and Authorization
 - ▶ Health Claims or Equivalent Encounter Information
 - ▶ Health Claim Status
 - ▶ Healthcare Payment and Remittance Advise
 - ▶ Coordination of Benefits
 - ▶ Eligibility for Health Plan
 - ▶ Health Plan Premium Payments
 - ▶ National Standards for Electronic Transactions
 - ▶ ANSI ASC X12N standards, Version 4010

Code Sets (October 2002 or 2003)

- 
- ▶ National Standard Code Sets
 - ▶ Diagnosis - ICD-9-CM (vol. 1 & 2)
 - ▶ Treatment Procedure Codes
 - ▶ CPT Codes
 - ▶ CDT Codes
 - ▶ ICD-9-CM (vol. 3) Codes, or
 - ▶ HCPCS Codes
 - ▶ Prescription Medications - NDC and J-Codes
 - ▶ All local treatment procedure codes will be eliminated
 - ▶ Most all DMH service codes and many Medicaid Codes are local codes

Potential Example Missouri DMH System



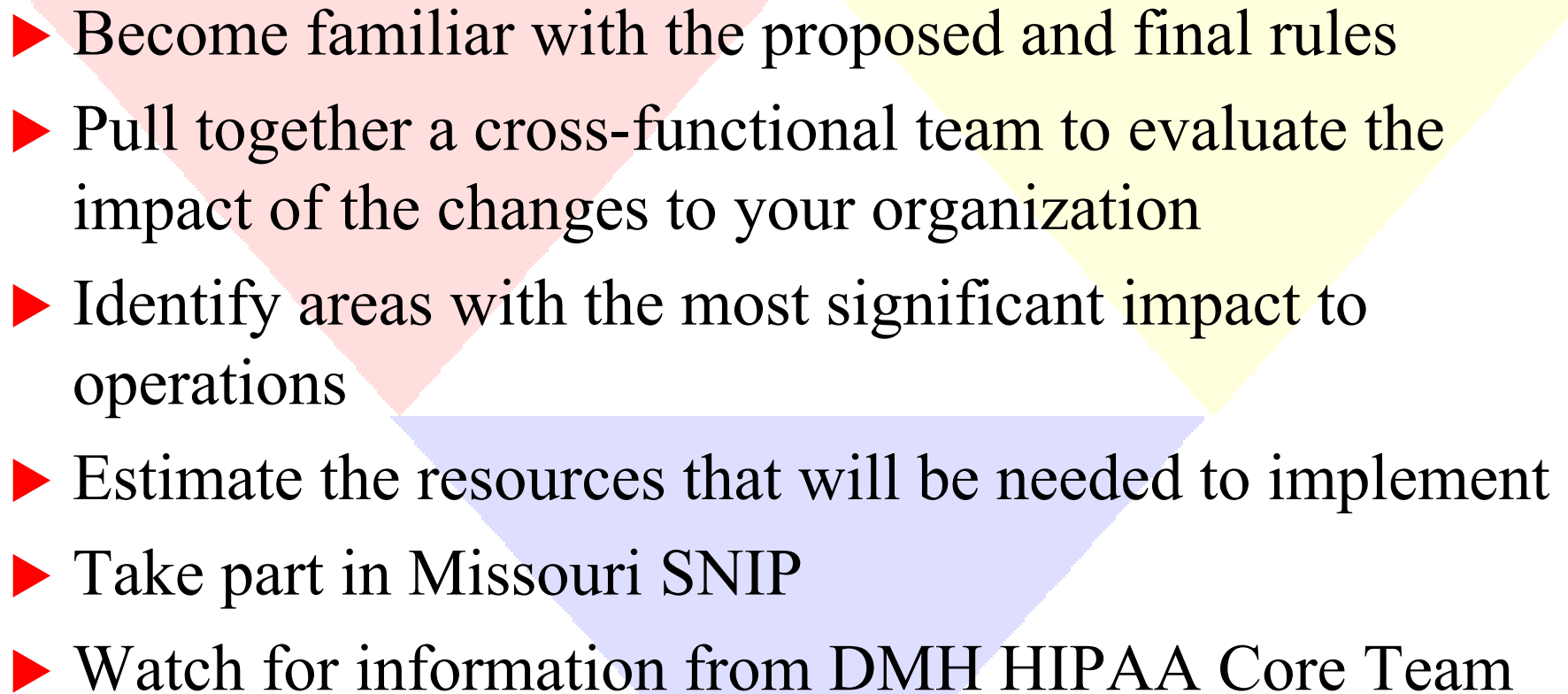
What is CIMOR?

- ▶ Customer Information Management, Outcomes and Reporting system
- ▶ DMH's initiative to replace current DMH central and facility information systems
- ▶ Will be accessible over the department's private network
- ▶ Is scheduled to be implemented July 2003

How CIMOR Will Help

- ▶ HIPAA Compliant Information System
 - ▶ Standard Transaction and Code Sets Capable Software
 - ▶ Standard Transactions and Code Sets built in as we know them
 - ▶ Privacy and Security Capable Software
- ▶ Statewide Implementation
 - ▶ HIPAA Compliant Claims by October 2003

Preparing for HIPAA

- 
- ▶ Become familiar with the proposed and final rules
 - ▶ Pull together a cross-functional team to evaluate the impact of the changes to your organization
 - ▶ Identify areas with the most significant impact to operations
 - ▶ Estimate the resources that will be needed to implement
 - ▶ Take part in Missouri SNIP
 - ▶ Watch for information from DMH HIPAA Core Team

Missouri SNIP

- ▶ Missouri Strategic National Implementation Process
 - ▶ Non-for-profit organization formed to meet the immediate need of developing an organized strategic implementation plan for a smooth implementation of the HIPAA legislation while maintaining healthy competition with our industry colleagues.
- ▶ Meets monthly in Columbia
 - ▶ \$200 Corporate Membership plus \$25 per person per meeting
- ▶ Membership includes state and private agencies
- ▶ Information - <http://www.mosnip.com/>

Questions for Software Vendors

From Ohio Department of Mental Health Web Site

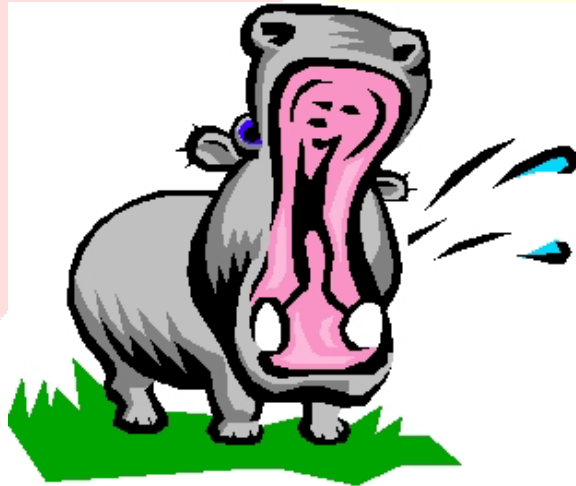
- ▶ How is the vendor preparing for HIPAA? (Who is leading the effort? How many resources are devoted to the project? Are they planning conferences/focus groups, etc?)
- ▶ What specifically will be included in the planned system modifications and when? (Ex. Which EDI Transactions, Code Sets, Security Features, etc.)
- ▶ What are the vendors contingency plans if they cannot deliver modifications before the required timeframe?
- ▶ What approach will the vendor use to meet HIPAA requirements (Ex. Will incoming data be converted from required ANSI standard format back to old proprietary format in a "behind-the-scenes" translation?)

Questions for Software Vendors

From Ohio Department of Mental Health Web Site

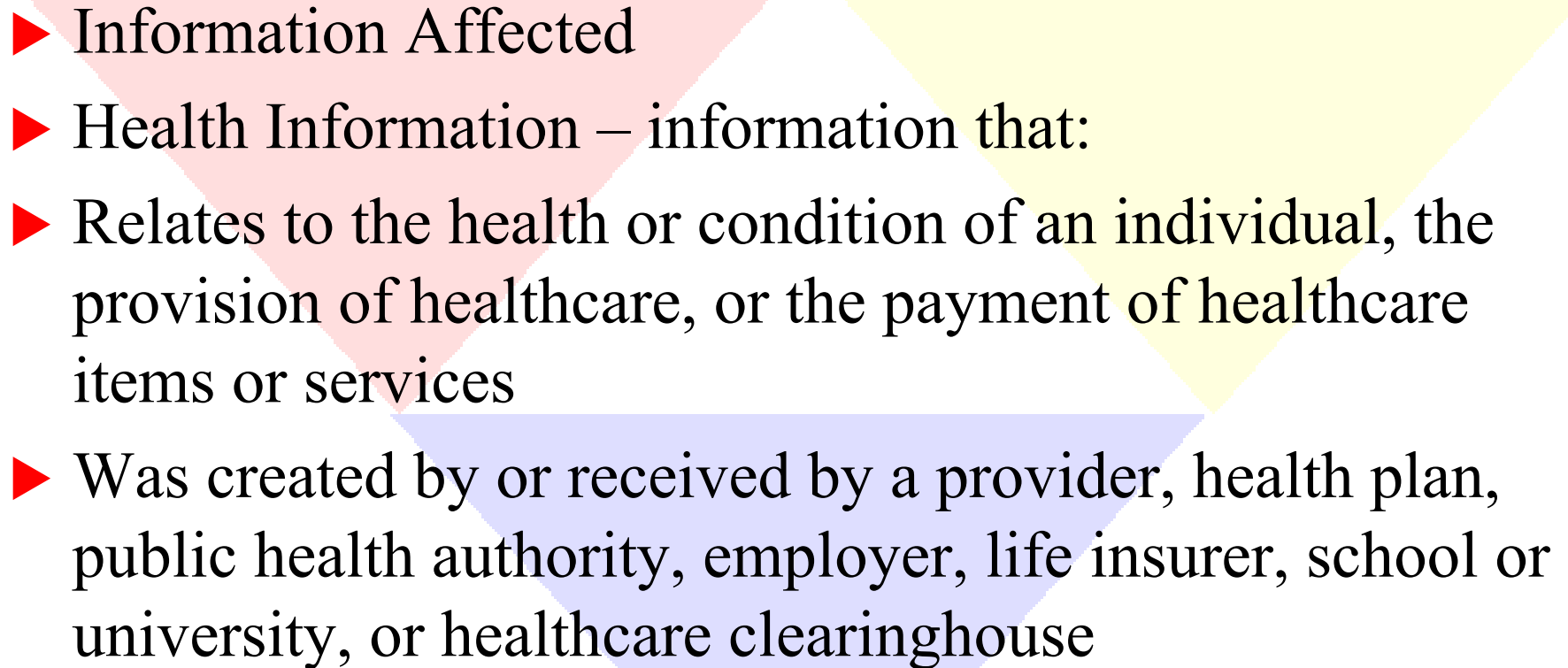
- ▶ What system modules or features will be affected? Will the changes require re-training? Will the changes affect existing custom reports or interfaces?
- ▶ Will the vendor provide enhanced security features to meet the HIPAA standards?
- ▶ What types of security features are the vendors considering?
- ▶ What will the added cost of the modifications be?
- ▶ What monitoring and audit capabilities does the software provide?
- ▶ For internet applications, does it have encryption strength that meets the HCFA Internet Policy?
- ▶ Does the encryption affect the system's performance?

Privacy: Keeping stuff to yourself



Dennis Hare & Kay Green
Division Mental Retardation &
Developmental Disabilities
Missouri Department of Mental Health

Privacy 101

- 
- ▶ Information Affected
 - ▶ Health Information – information that:
 - ▶ Relates to the health or condition of an individual, the provision of healthcare, or the payment of healthcare items or services
 - ▶ Was created by or received by a provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse

What Information Is Affected?

- ▶ Privacy rules relate to both electronic and paper records, and oral communications
- ▶ Standards apply to:
 - ▶ Transmission by internet, intranets, leased lines, dial-up lines, private networks
 - ▶ Includes physical movement of data on diskette, CD, magnetic tape, etc.

How Did Privacy Happen?

- ▶ How did this all come about?
- ▶ Purpose
 - ▶ To improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals.
- ▶ “Privacy is a fundamental right...it speaks to our individual and collective freedoms”. (Federal Register, Vol. 65, p. 82464).

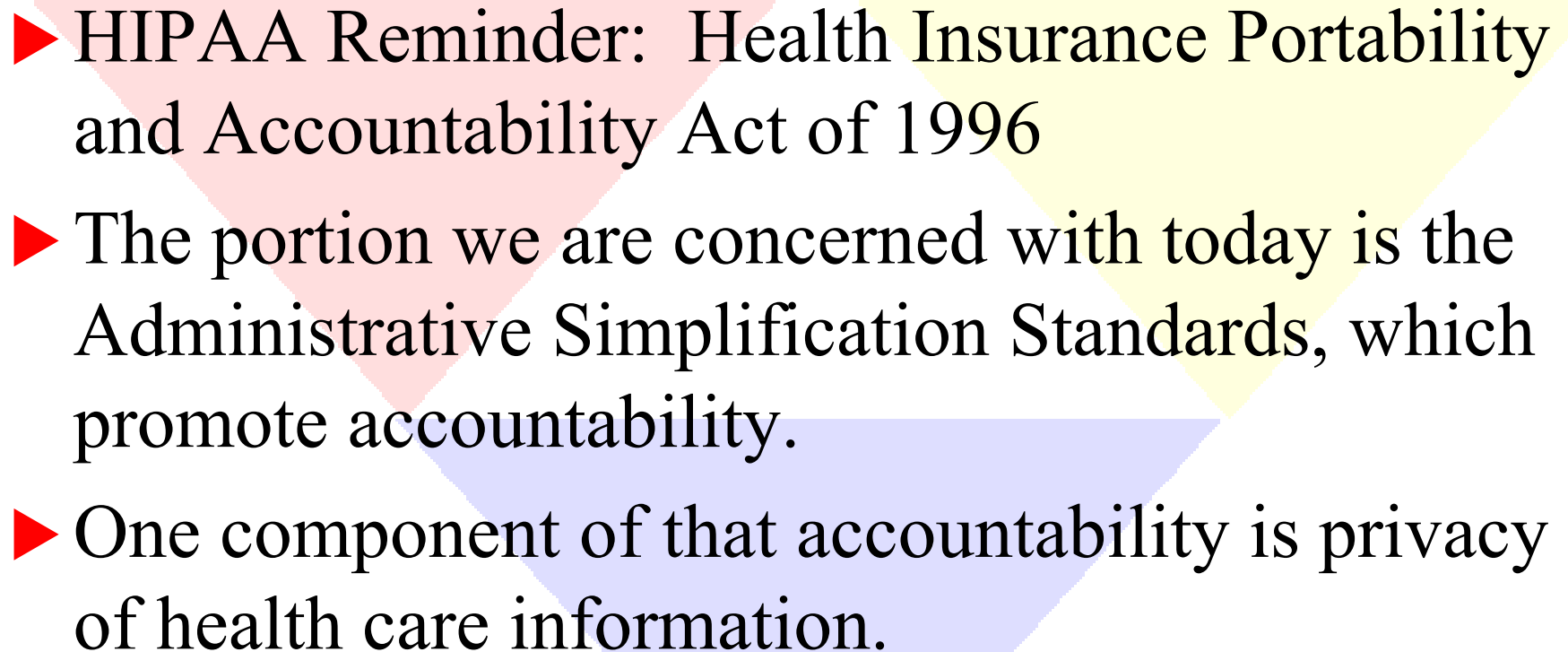
How Did Privacy Happen?

- ▶ There was an increasing public concern about loss of privacy.
- ▶ There was an increasing use of interconnected electronic information systems.
- ▶ There are many advances in genetic science.
- ▶ The determination that privacy is necessary to secure effective, high quality health care.
- ▶ Are there examples of privacy breaches?

Privacy Breaches

- ▶ A banker who sat on a county's health board accessed patient's health records, identified several people with cancer and called in their mortgages.
- ▶ A physician was diagnosed with AIDS at the hospital in which he practiced medicine. His surgical privileges were suspended.
- ▶ A candidate for congress nearly saw her campaign derailed when facts of her psychiatric treatment and suicide attempt were published in the NY Times.
- ▶ An Illinois woman whose photo and medical records were posted to the Internet by anti-abortion activists after she underwent an abortion was embarrassed and subject to public ridicule.
- ▶ Many may remember when Senator Eagleton was replaced on the Democratic ticket because his treatment of depression was surreptitiously released to the newspapers.

Privacy Basics

- 
- ▶ HIPAA Reminder: Health Insurance Portability and Accountability Act of 1996
 - ▶ The portion we are concerned with today is the Administrative Simplification Standards, which promote accountability.
 - ▶ One component of that accountability is privacy of health care information.

Privacy Basics



▶ Privacy

- ▶ How you use or disclose data
- ▶ Use: within covered entity
- ▶ Disclose: release of data outside the entity

▶ Security

- ▶ How you store or transmit data

Privacy Implementation

- ▶ Is it really happening?
 - ▶ Final Privacy Rule established April 2001
 - ▶ Final Modifications issued August 14, 2002.
 - ▶ Current mandatory compliance date: April 14, 2003
 - ▶ Supported (so far) by both Clinton and Bush administrations
 - ▶ May or may not have legislative extension requests

Privacy Implementation

- 
- ▶ Assume you need to assure compliance by **April 14, 2003!!!**

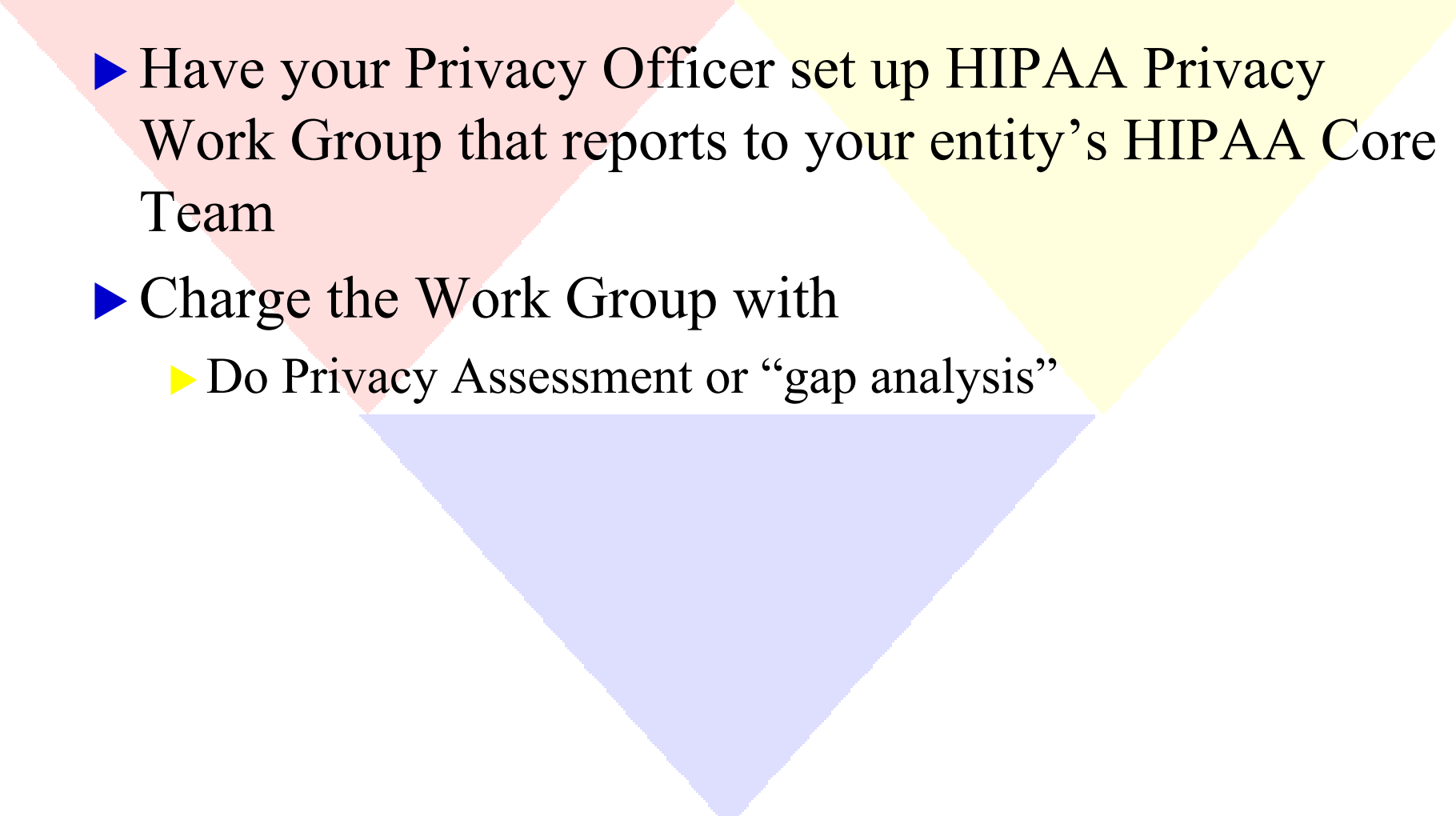
Privacy Officer Functions

- ▶ Designate a Privacy Officer for each covered entity
- ▶ That person should oversee all ongoing activities related to the development, implementation, maintenance of, and adherence to the entity's privacy policies and procedures.
- ▶ Should also conduct periodic audits and construct a monitoring trail.

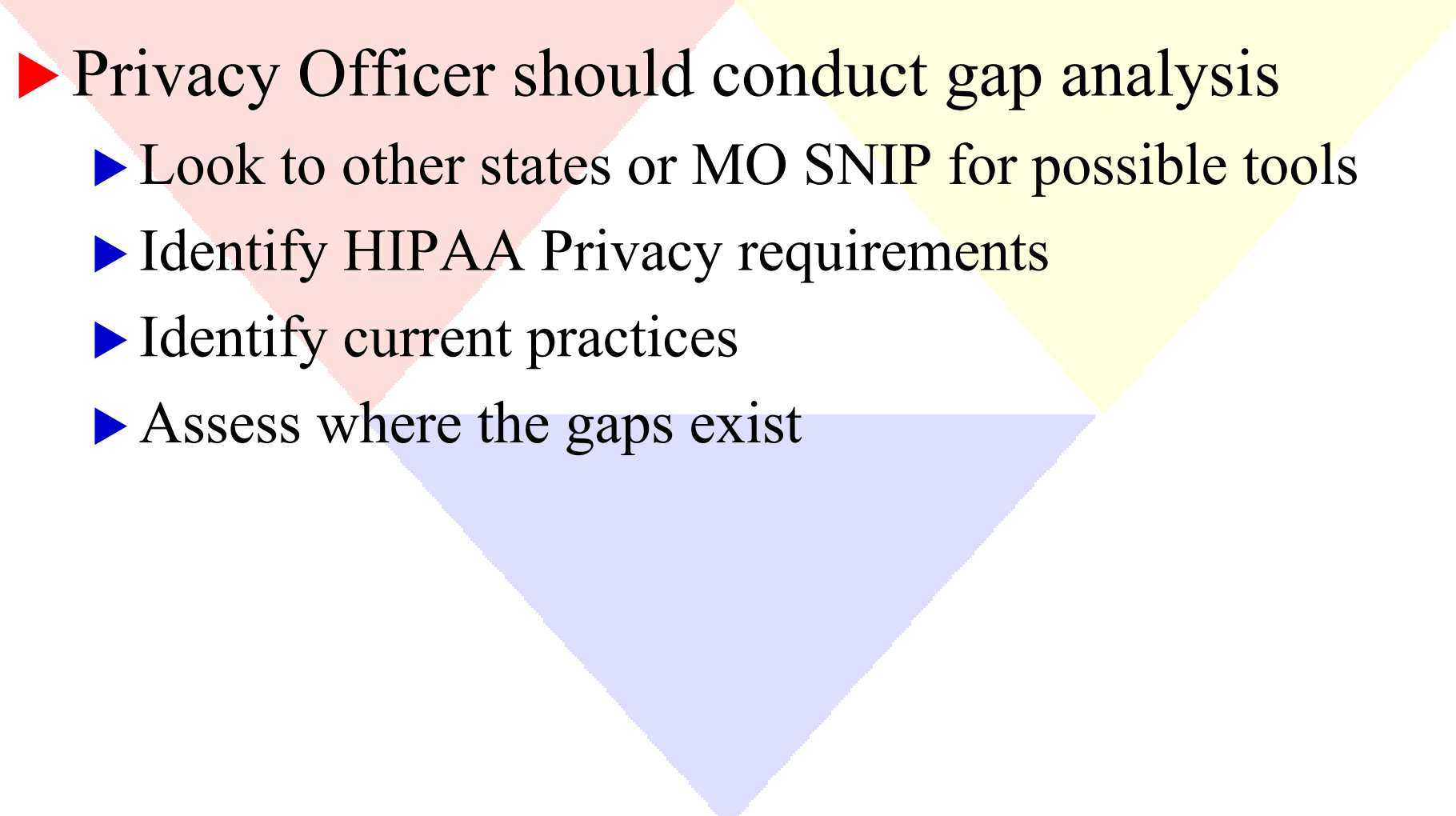
Privacy Officer Functions

- ▶ What should a Privacy Officer do?
 - ▶ Pull together a cross-functional team to evaluate the impact of HIPAA changes
 - ▶ Become familiar with final rule and modifications
 - ▶ Identify areas with most significant impact to operations
 - ▶ Watch for information from DMH HIPAA Core Team: www.modmh.state.mo.us
 - ▶ Take part in Missouri SNIP

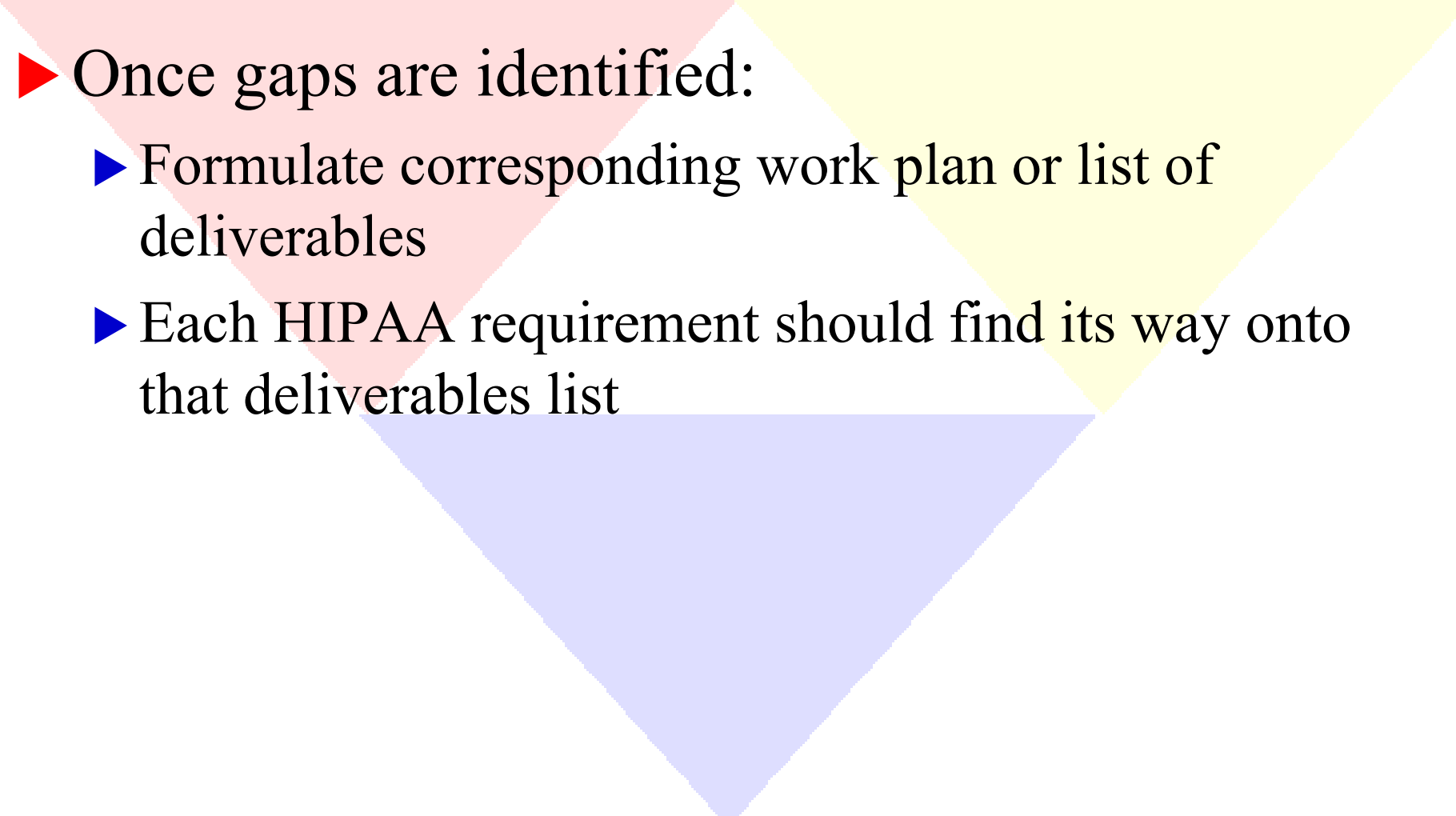
Privacy Officer Functions

- 
- ▶ Have your Privacy Officer set up HIPAA Privacy Work Group that reports to your entity's HIPAA Core Team
 - ▶ Charge the Work Group with
 - ▶ Do Privacy Assessment or “gap analysis”

Privacy Officer Functions

- 
- ▶ Privacy Officer should conduct gap analysis
 - ▶ Look to other states or MO SNIP for possible tools
 - ▶ Identify HIPAA Privacy requirements
 - ▶ Identify current practices
 - ▶ Assess where the gaps exist

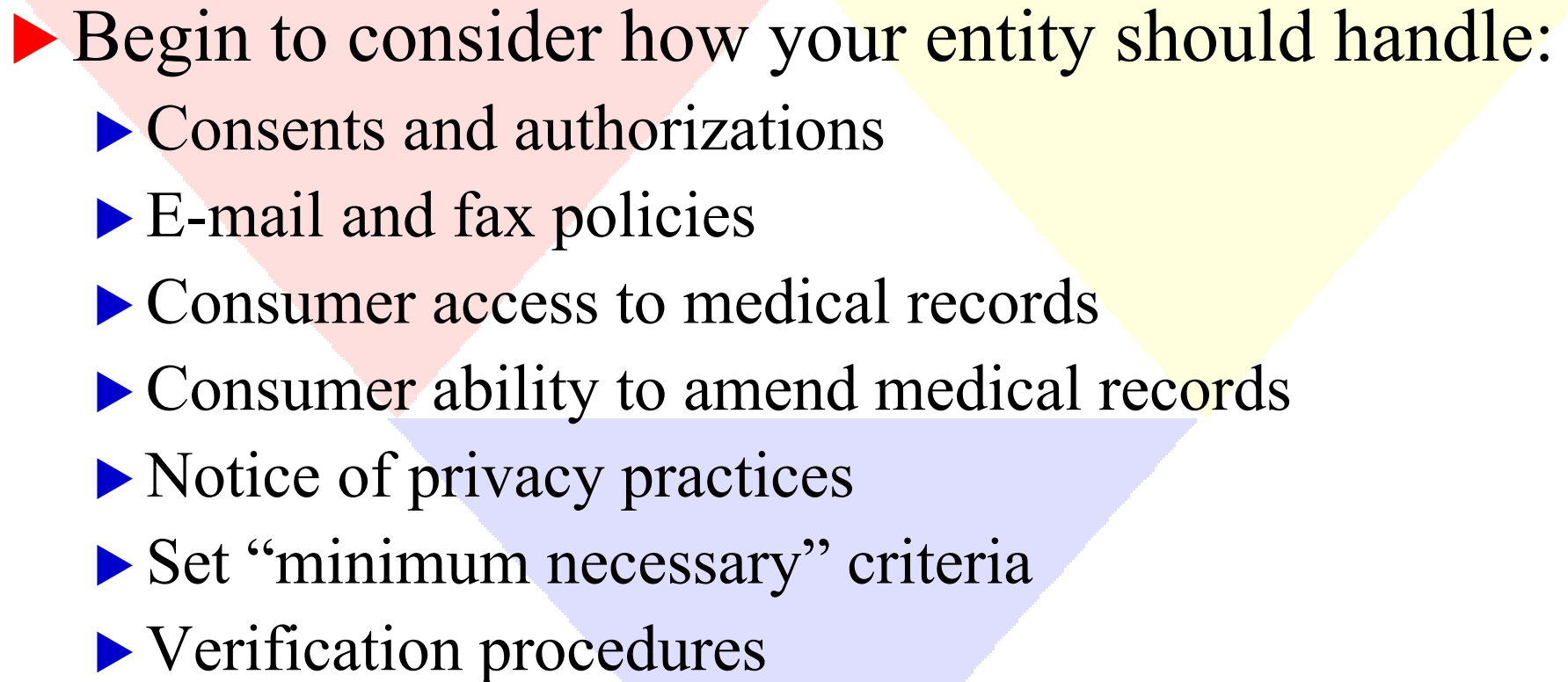
Privacy Officer Functions

- 
- ▶ Once gaps are identified:
 - ▶ Formulate corresponding work plan or list of deliverables
 - ▶ Each HIPAA requirement should find its way onto that deliverables list

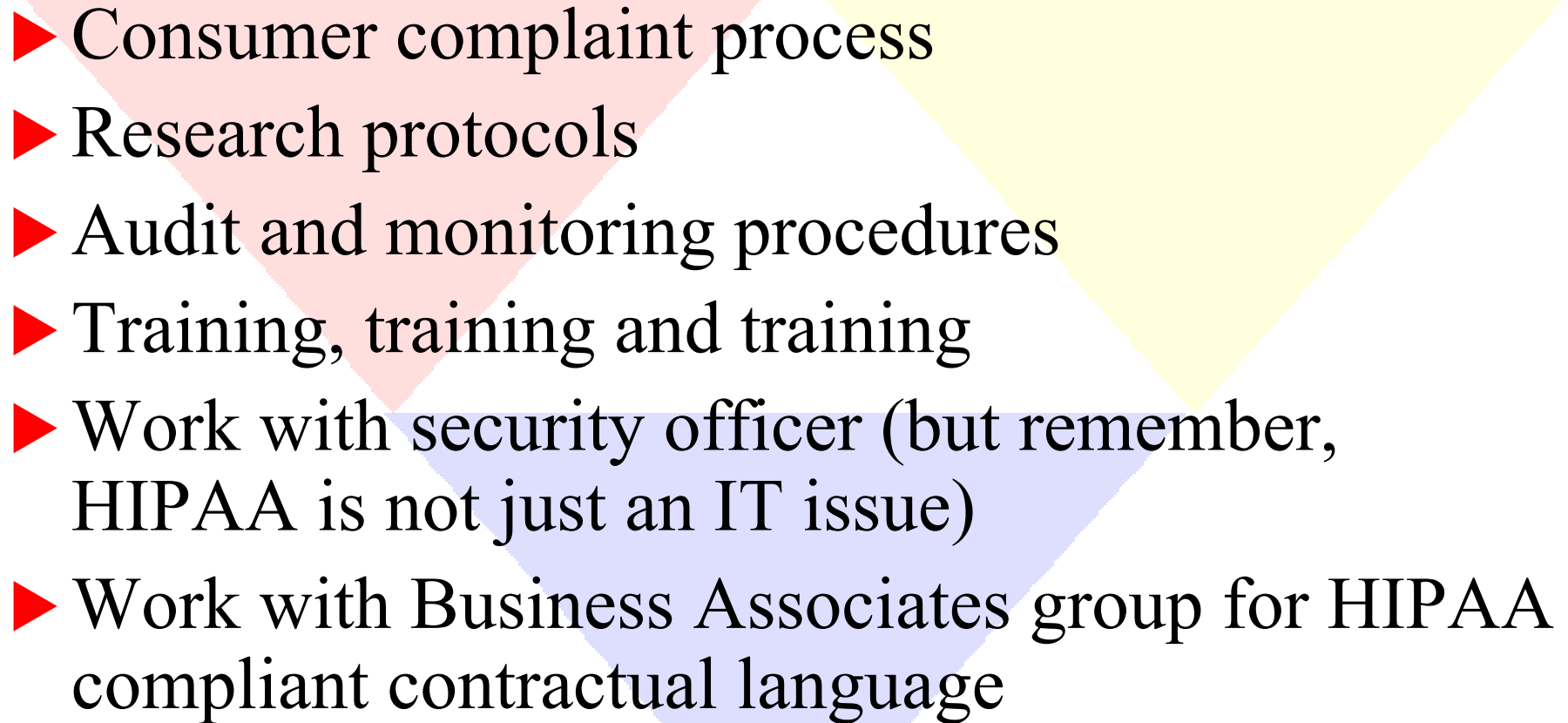
Privacy Officer Functions

- ▶ Privacy Officer should then identify each location in your organization where PHI (protected health information) resides
- ▶ Then, further identify who uses that PHI within your organization; or who makes requests for disclosures; and which of your staff responds to those requests.
- ▶ Work with your legal counsel to determine how all laws work together (which state laws are preempted and which ones are not).

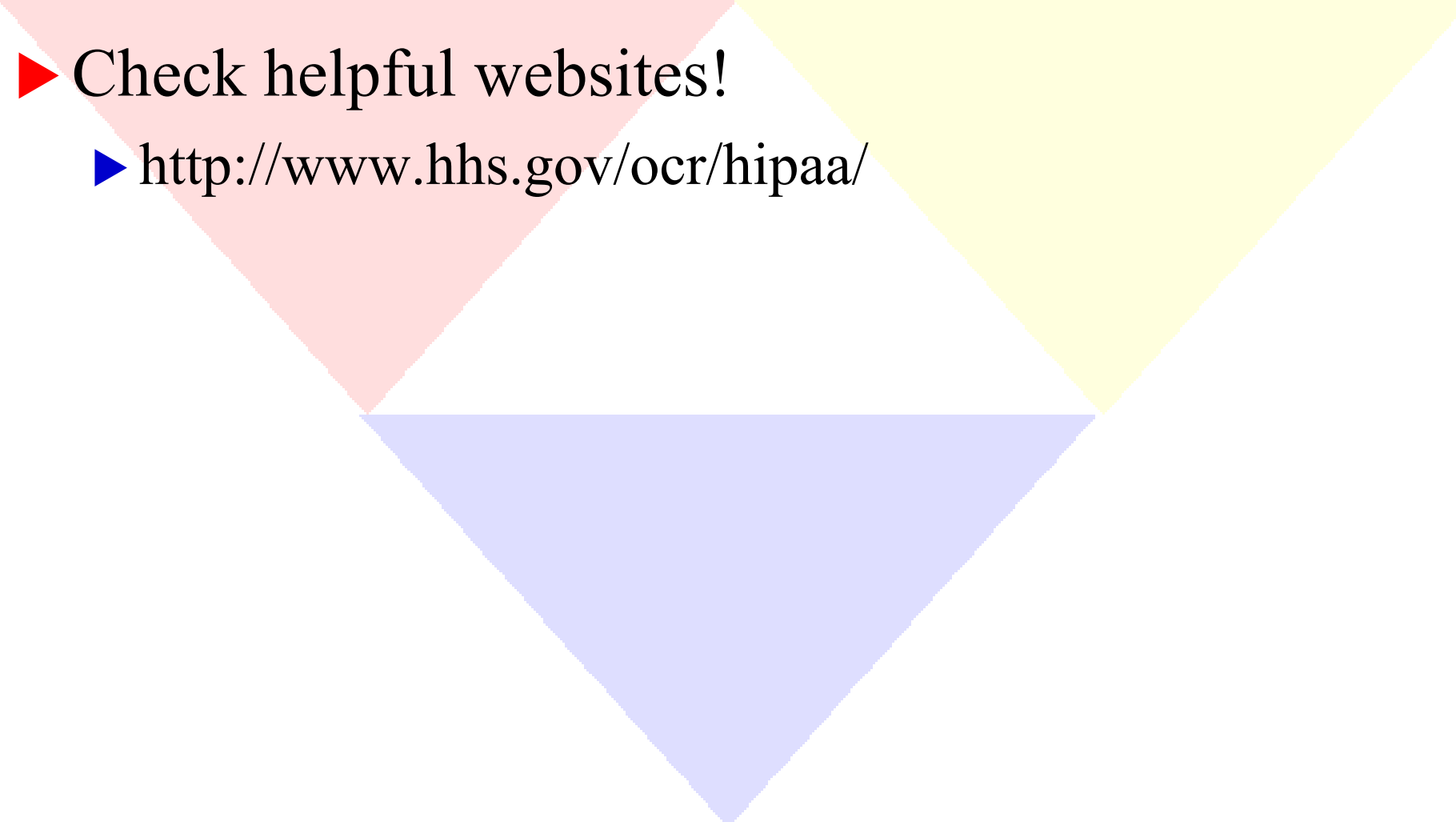
Privacy Officer Functions

- 
- ▶ Begin to consider how your entity should handle:
 - ▶ Consents and authorizations
 - ▶ E-mail and fax policies
 - ▶ Consumer access to medical records
 - ▶ Consumer ability to amend medical records
 - ▶ Notice of privacy practices
 - ▶ Set “minimum necessary” criteria
 - ▶ Verification procedures

Privacy Officer Functions

- 
- ▶ Consumer complaint process
 - ▶ Research protocols
 - ▶ Audit and monitoring procedures
 - ▶ Training, training and training
 - ▶ Work with security officer (but remember, HIPAA is not just an IT issue)
 - ▶ Work with Business Associates group for HIPAA compliant contractual language

Privacy Officer Functions

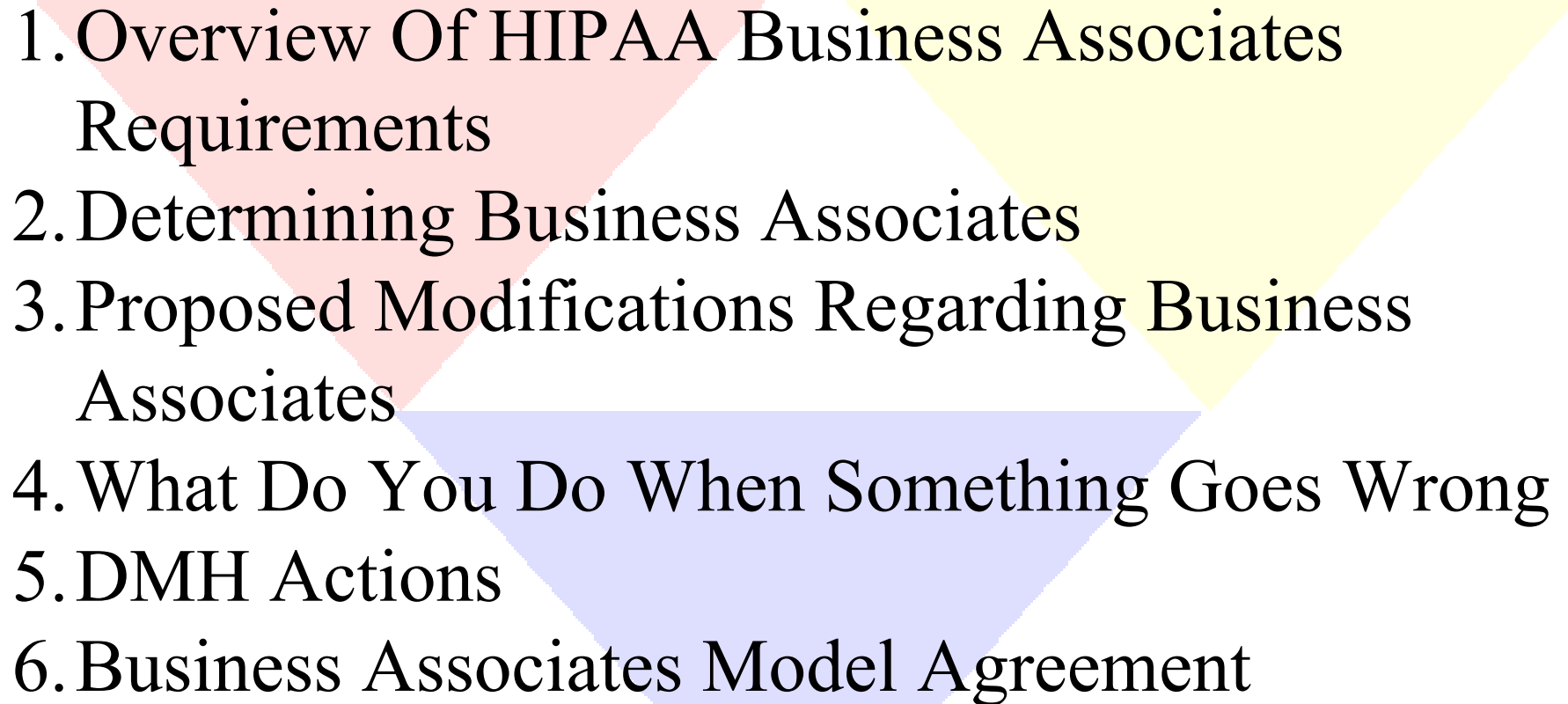
- 
- ▶ Check helpful websites!
 - ▶ <http://www.hhs.gov/ocr/hipaa/>

Business Associates: Sharing stuff



Pam Leyhe & Loren Israel
Missouri Department of Mental Health

Workshop Goals

- 
1. Overview Of HIPAA Business Associates Requirements
 2. Determining Business Associates
 3. Proposed Modifications Regarding Business Associates
 4. What Do You Do When Something Goes Wrong
 5. DMH Actions
 6. Business Associates Model Agreement

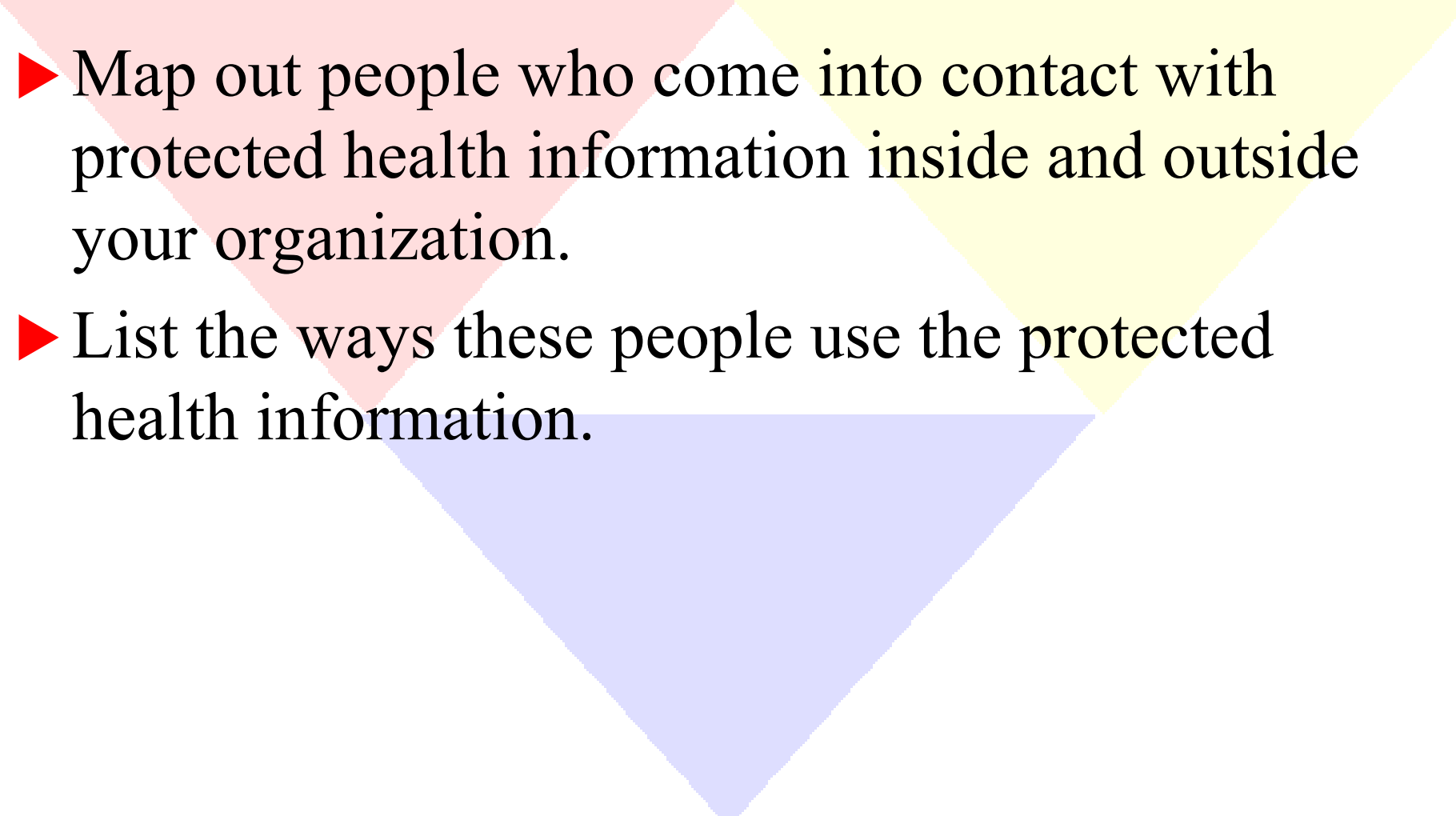
Why was there concern about Business Associates?

- ▶ Most health care providers do not work by themselves.
- ▶ To complete the tasks required of them, identifiable health information must be passed along.
- ▶ HHS recognized for identifiable health information to be truly protected, the distribution and use of such information by the business associates had to be restricted.

What or whom is a Business Associate?

- ▶ A person to whom the covered entity discloses protected health information so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity.

Identification of Business Associates

- 
- ▶ Map out people who come into contact with protected health information inside and outside your organization.
 - ▶ List the ways these people use the protected health information.

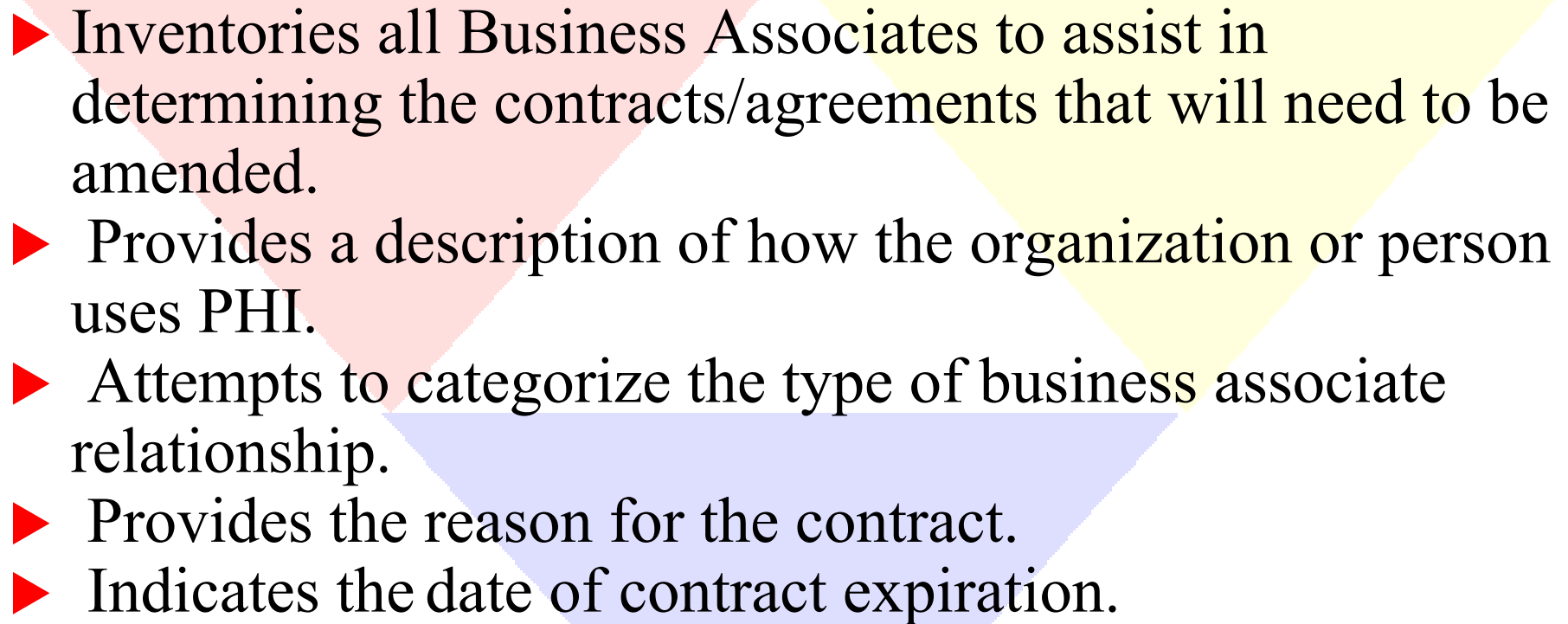
Business Associates: Who's Handling Your Patients' Information

- ▶ Many organizations may have access to your patients' data for a variety of reasons unrelated to direct healthcare.
- ▶ Billing Services
- ▶ Computer Technicians
- ▶ Lawyers
- ▶ Accountants

Business Associates: Who's Handling Your Patients' Information, Cont.

- 
- ▶ Auditors
 - ▶ Health Care Consultants
 - ▶ Law Enforcement Officials
 - ▶ Mailing Services
 - ▶ Software Vendors
 - ▶ Advocacy Groups / Associations

DMH HIPAA Business Associates Tool

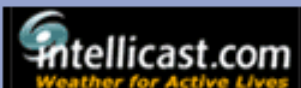
- 
- ▶ Inventories all Business Associates to assist in determining the contracts/agreements that will need to be amended.
 - ▶ Provides a description of how the organization or person uses PHI.
 - ▶ Attempts to categorize the type of business associate relationship.
 - ▶ Provides the reason for the contract.
 - ▶ Indicates the date of contract expiration.

- DMH-Online ▶
- Employee Information ▶
- Department ▶
- Divisions ▶
- Offices ▶
- Resources ▶
- Applications ▶

Search DMH-Online

Search!

Clear



Zip Code/City Search



HIPAA Business Associates Tool - Matrix Display

[Add New](#)

[Business Associate](#)

Action	Business Associate	Expires	Last Updated
	Accountants	10/31/2003	03/15/2002
	Accreditation services	07/31/2002	03/06/2002
	Chiropractors	06/30/2003	03/05/2002
	Dentists	01/31/2002	03/06/2002
	test	04/30/2002	03/15/2002

View Another Facility:

Central Office

[Business Associates Home](#)

[HIPAA Home](#) | [Department Home](#) | [DMH-Online Home](#)

Search DMH-OnLine



Zip Code/City Search

[DMH Internet Site](#)
[State Home Page](#)

HIPAA Business Associates On-Line

Division: *CO* User: *mzleyhp* Facility: *Central Office*Business Associate: Other: **Description of Health Data Exchange****Type of BA Relationship**

- | | |
|---|---|
| <input type="radio"/> Incidental Contact | <input type="radio"/> Existing Contract |
| <input type="radio"/> Key Business Associates | <input type="radio"/> Volunteers |
| <input type="radio"/> Other Government Entities | <input type="radio"/> Advocacy Groups |

Contract:

- ☐
- Yes
- ☐
- No

Reason For Contract**Agreement:**

- ☐
- Written
-
- ☐
- Oral

Contract Expiration

After Identification of Business Associates, What Do You Need to Do?

- ▶ The privacy rule mandates that covered entities must have business associate contracts or agreements with all organizations and individuals they work with that have access to or use protected health information to assist or perform a function for the covered entity.
- ▶ The privacy rule requires that the satisfactory assurances obtained from the business associate be in the form of a written contract (or other written arrangement).

After Identification of Business Associates, What Do You Need to Do, Cont.

- ▶ The agreement must identify the uses and disclosures of protected health information the business associate is permitted or required to make, as well as require the business associate to put into place appropriate safeguards to protect against a use or disclosure not permitted by the contract or agreement.

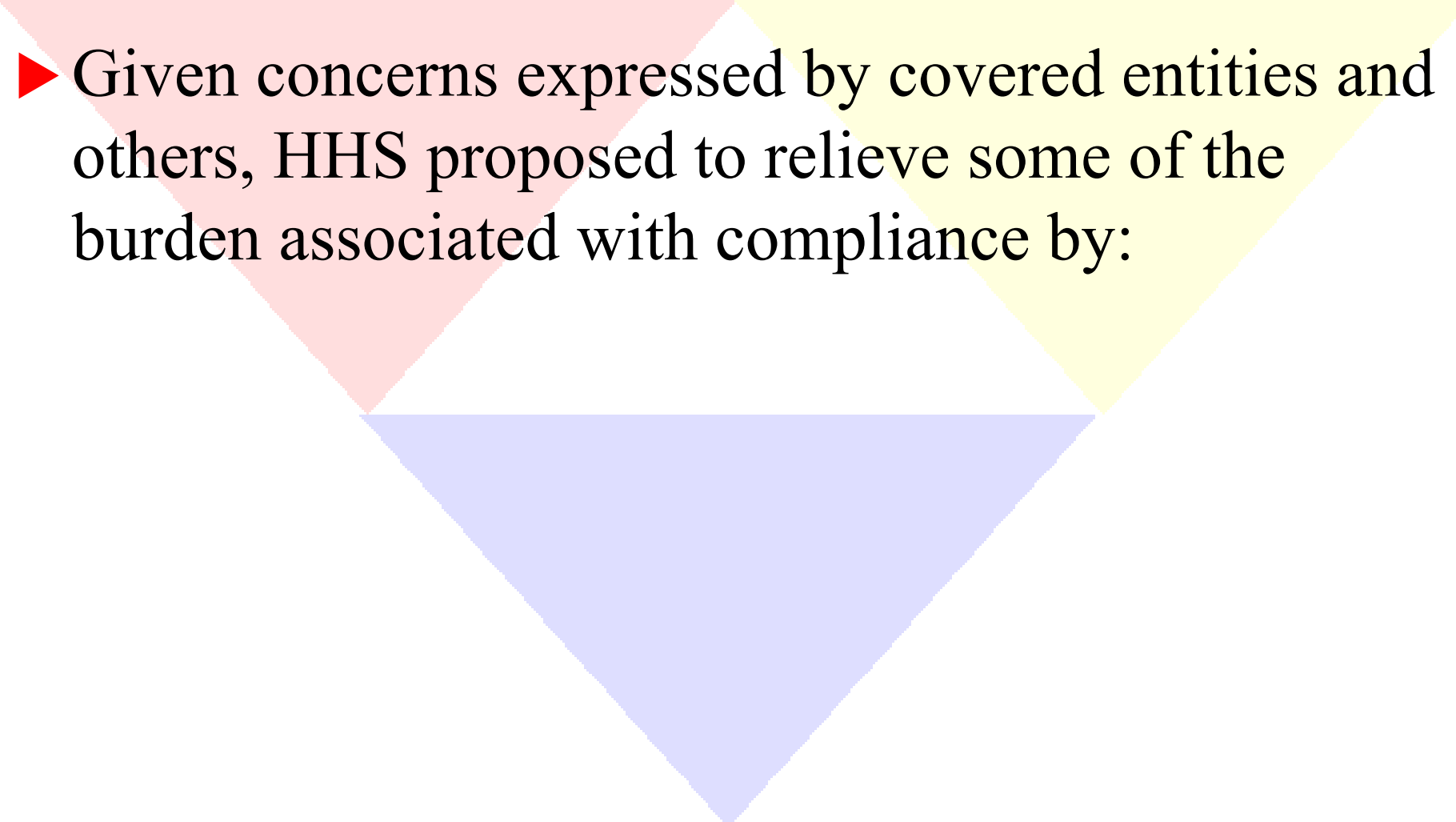
When Business Associate Contracts are Required

- ▶ Disclosing protected health information to another entity that will use the information on behalf of the covered entity.
- ▶ When Business Associate will be or are obtaining protected health information on behalf of the covered entity.
- ▶ When Business Associate is providing specific services to the covered entity involving the disclosure of information by the covered entity to the Business Associate.

The Good News?

- ▶ August, 2002 – HHS issued the set of final modifications to the previously published HIPAA regulations.
- ▶ The model provisions can be found at:
<http://www.hipaadvisory.com/regs/privacynprm/modelba.htm>

The Good News, Continued

- 
- ▶ Given concerns expressed by covered entities and others, HHS proposed to relieve some of the burden associated with compliance by:

The Good News, Continued

- ▶ Allowing covered entities, other than small group plans, to continue to operate under certain existing contracts with business associates for up to one year beyond the April 14, 2003 compliance date. HHS deemed the contracts to be compliant with the Privacy Rule until either the covered entity had renewed or modified the contract following the compliance date (April 14, 2003), or April 14, 2004, whichever was sooner.
- ▶ In cases where a contract automatically renews, evergreen contracts, these are eligible for the extension.
- ▶ Extension applies only to written contracts or agreements, not to oral contracts or other arrangements.
- ▶ Providing sample business associate contract language.

The Good News: Proposed Modifications

- ▶ You do not have to use the model provisions.
- ▶ You can amend the model provisions to meet your needs.
- ▶ You can have freestanding agreements or amend contracts.
- ▶ Whatever you do, remember that the model agreement is written to address business associate requirements only.

Legalese Comments About The Proposed Modifications

- ▶ Suggestion: If your agency is creating a stand-alone Business Associates Agreement, as opposed to amending a current contract, you should confirm with your attorney that your document complies with Missouri's contracting requirements.
- ▶ Suggestion: Be sure to review the final modifications to ensure your agreement conforms with any amendments that may have been made to the model Business Associate Agreements.

Violations By a Business Associate

- ▶ If a covered entity knows of a material breach or violation by the business associate, the covered entity is required to take reasonable steps to cure the breach or end the violation.
- ▶ If this action is not successful, steps must be taken to terminate the contract or agreement.
- ▶ If termination of the contract or agreement is not feasible, a covered entity must report the problem to the Secretary of HHS.

What Can You Expect From DMH?

▶ HIPAA Placeholder Language

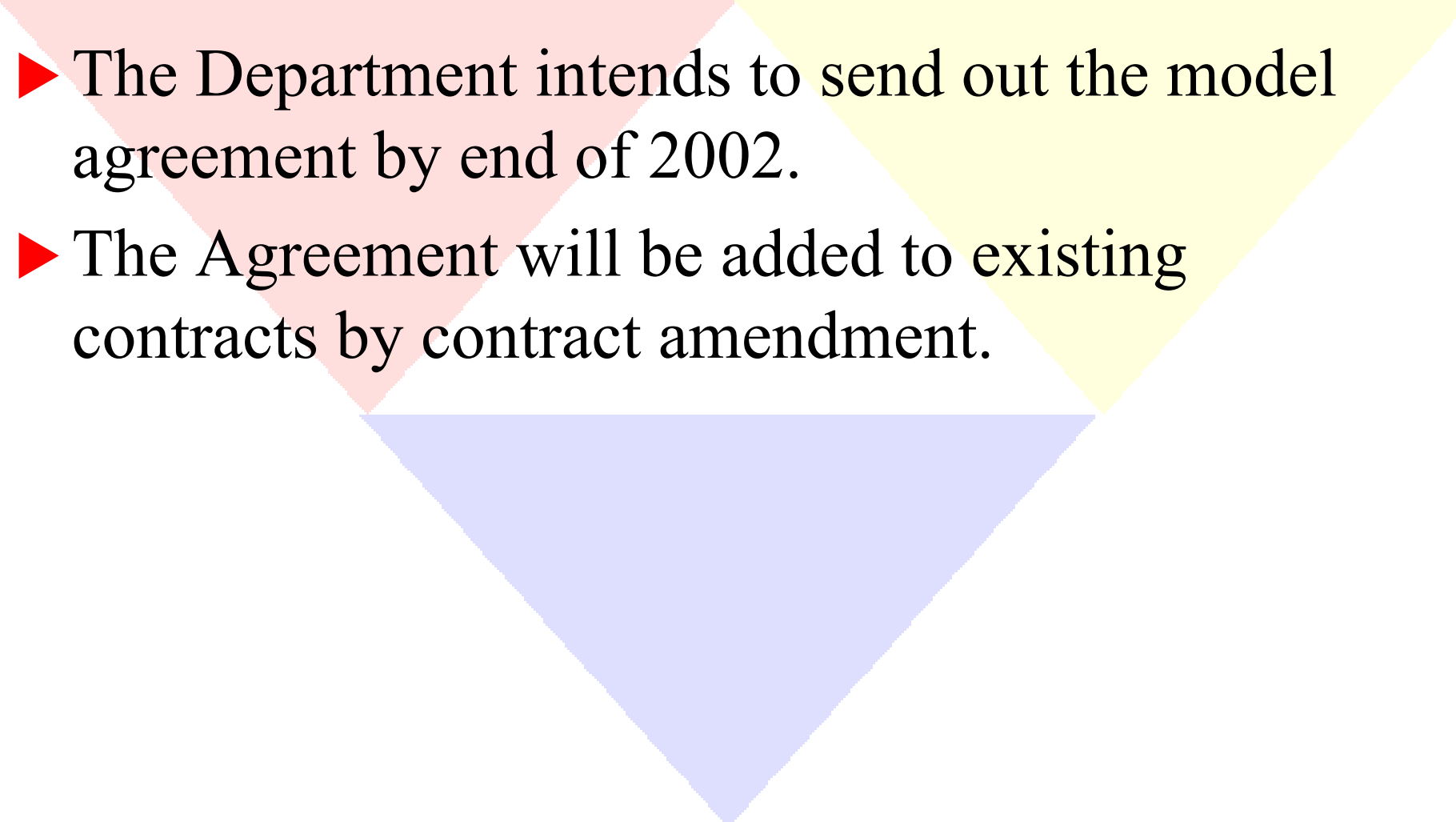
▶ Each party agrees to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as well as any federal rules and regulations pertaining to HIPAA. The parties agree that they will enter into any additional agreements required by HIPAA and its rules and regulations (for instance, business associate agreements) or will agree to amend this Agreement to include all necessary language to comply with all such requirements. The parties agree that these additional agreements or amendments may be negotiated and entered into at any time and that said additional agreements or amendments shall not effect the status or effective date of this Agreement.

What Can You Expect From DMH, Continued

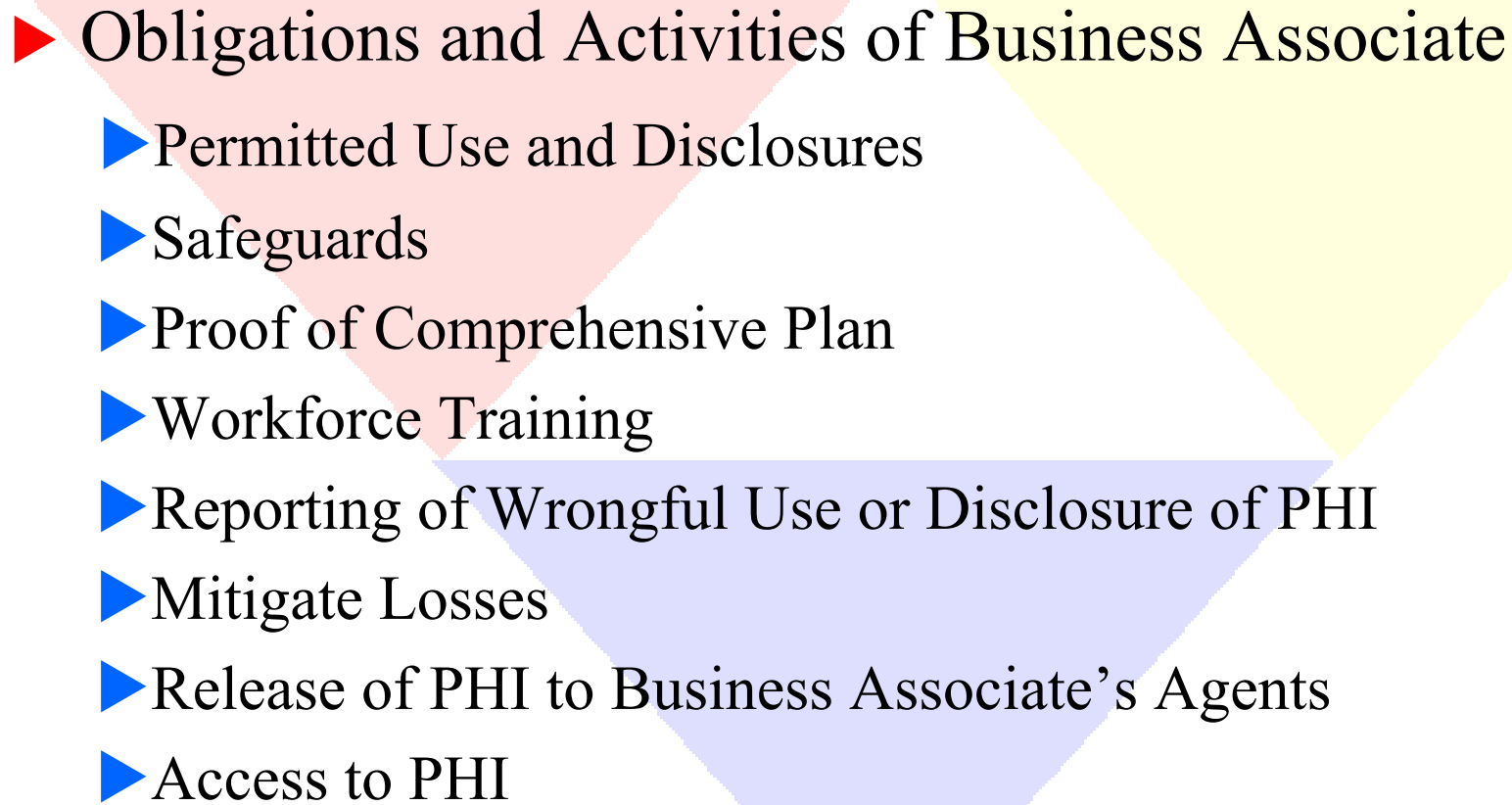
Such additional agreements or amendments shall be entered into on or before the date either party is required to be in compliance with HIPAA or its rules or regulations.

- ▶ There will be a mass mailing of this language to all contractors this fall.
- ▶ Provides notice that additional requirements are forthcoming to business associates.

Model Agreement: DMH Action

- 
- ▶ The Department intends to send out the model agreement by end of 2002.
 - ▶ The Agreement will be added to existing contracts by contract amendment.

Business Associate Model Agreement

- 
- ▶ Obligations and Activities of Business Associate
 - ▶ Permitted Use and Disclosures
 - ▶ Safeguards
 - ▶ Proof of Comprehensive Plan
 - ▶ Workforce Training
 - ▶ Reporting of Wrongful Use or Disclosure of PHI
 - ▶ Mitigate Losses
 - ▶ Release of PHI to Business Associate's Agents
 - ▶ Access to PHI

Permitted Uses and Disclosures by Business Associates

- ▶ Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI on behalf of, or to provide services to, Covered Entity for the following purposes, so long as such use of disclosures would not violate HIPAA or the HIPAA regulations if performed by the Covered Entity.

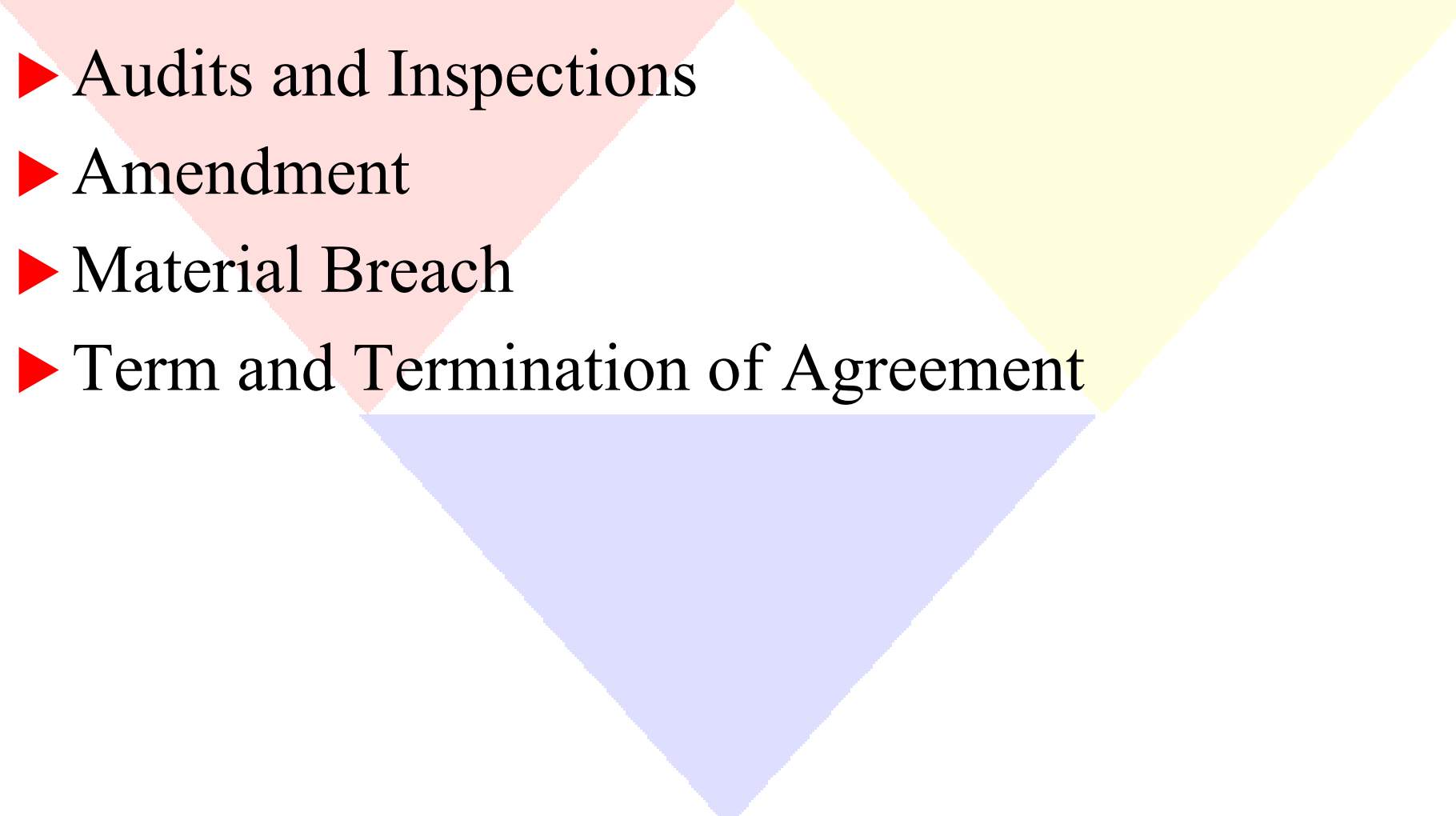
Obligations of Covered Entity

- ▶ Covered Entity agrees to be responsible for using appropriate safeguards to maintain and ensure the confidentiality, privacy and security of PHI transmitted to Business Associate.
- ▶ Covered Entity agrees to provide Business Associate with the notice of privacy practices.
- ▶ Covered Entity agrees to provide Business Associate with any changes in, or revocation of, permission by Individual to use or disclose PHI, if such changes affect Business Associate's permitted use and disclosures.

Obligations of Covered Entity, Continued

- ▶ Covered Entity agrees to notify Business Associate of any restrictions to the use or disclosure of PHI that Covered Entity has agreed to.
- ▶ Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule.

Other Sections of the Model Agreement

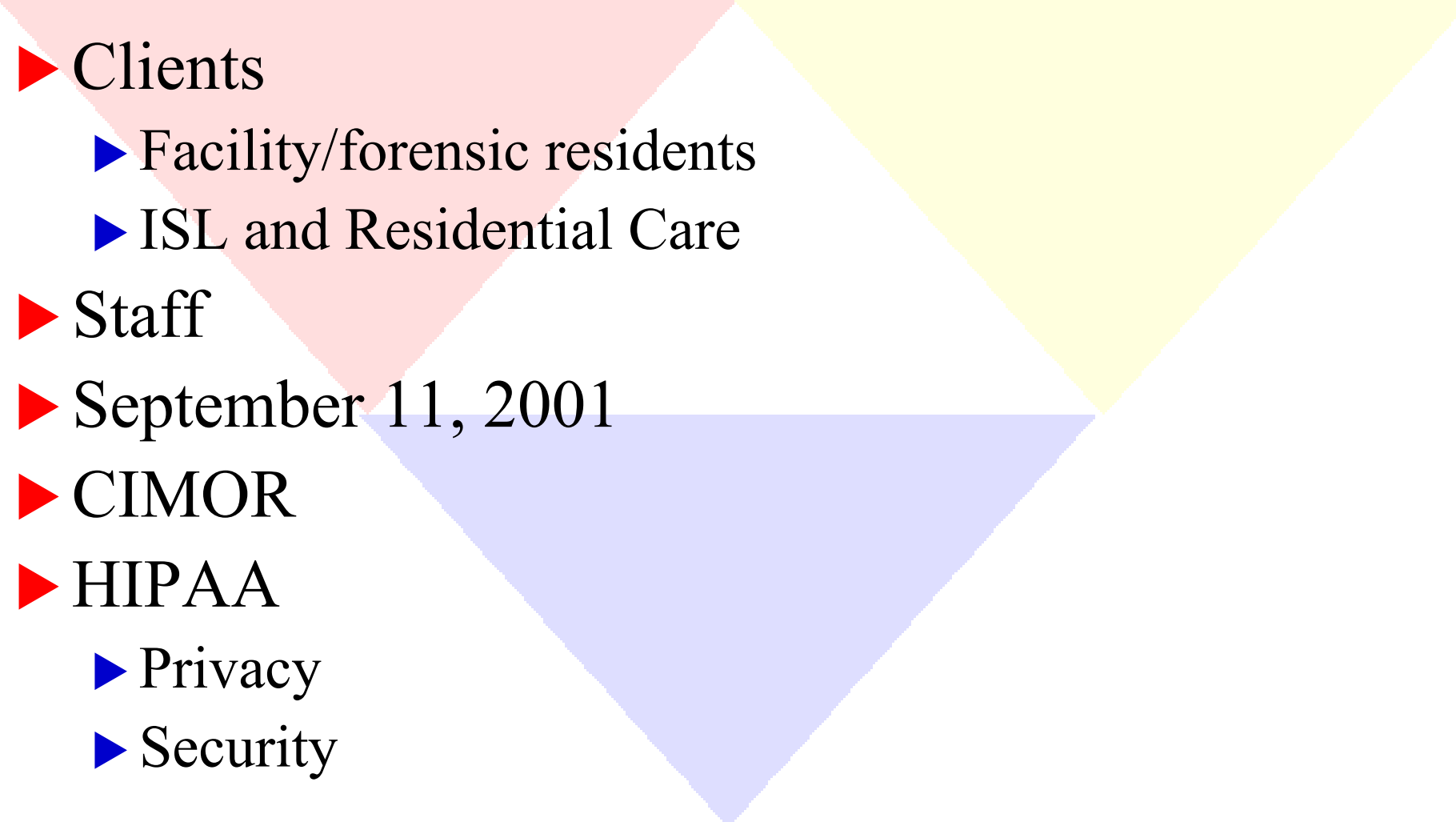
- 
- ▶ Audits and Inspections
 - ▶ Amendment
 - ▶ Material Breach
 - ▶ Term and Termination of Agreement

Security: Protecting stuff

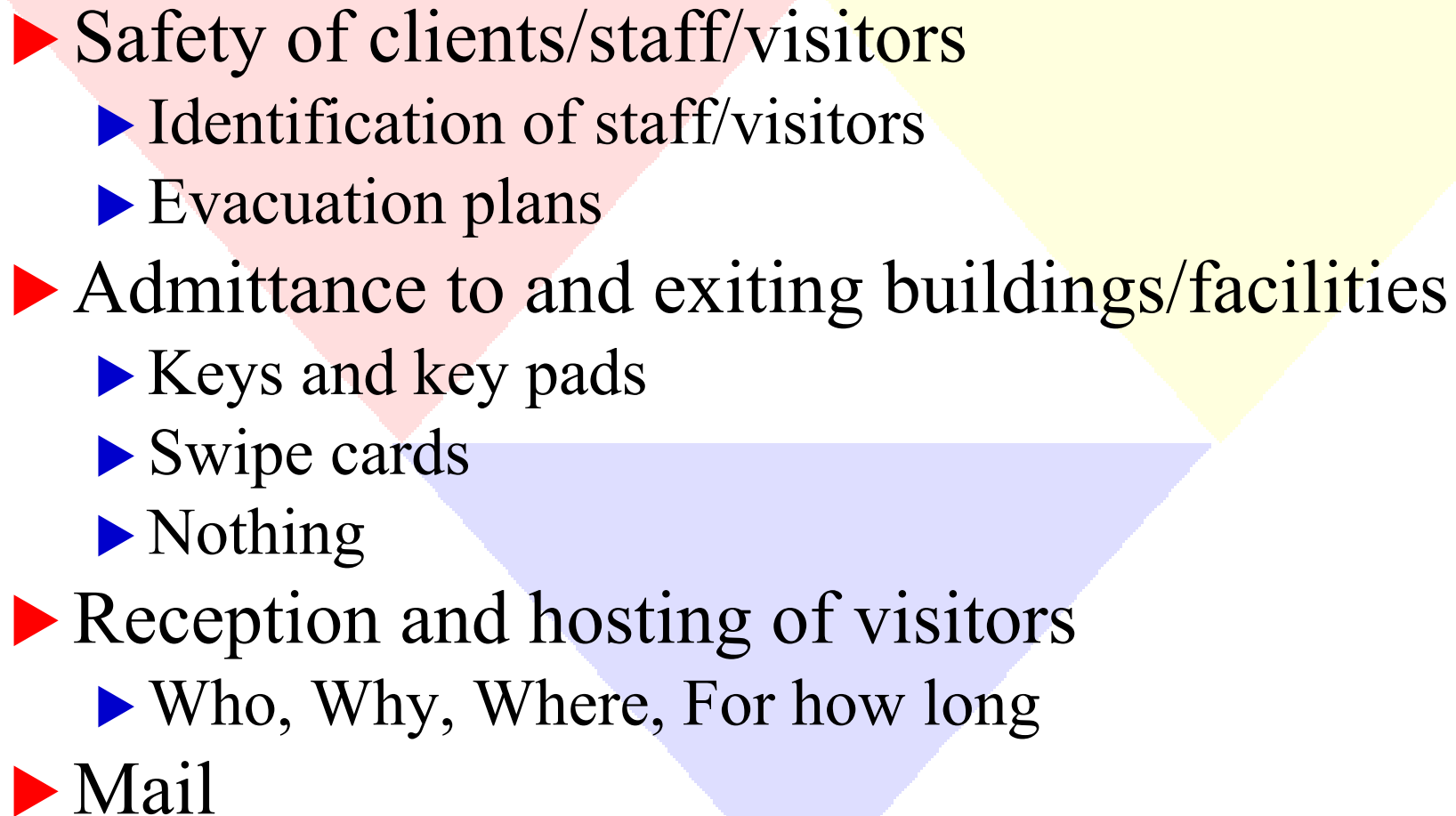


Dean Williams
Office of Information Systems
Missouri Department of Mental Health

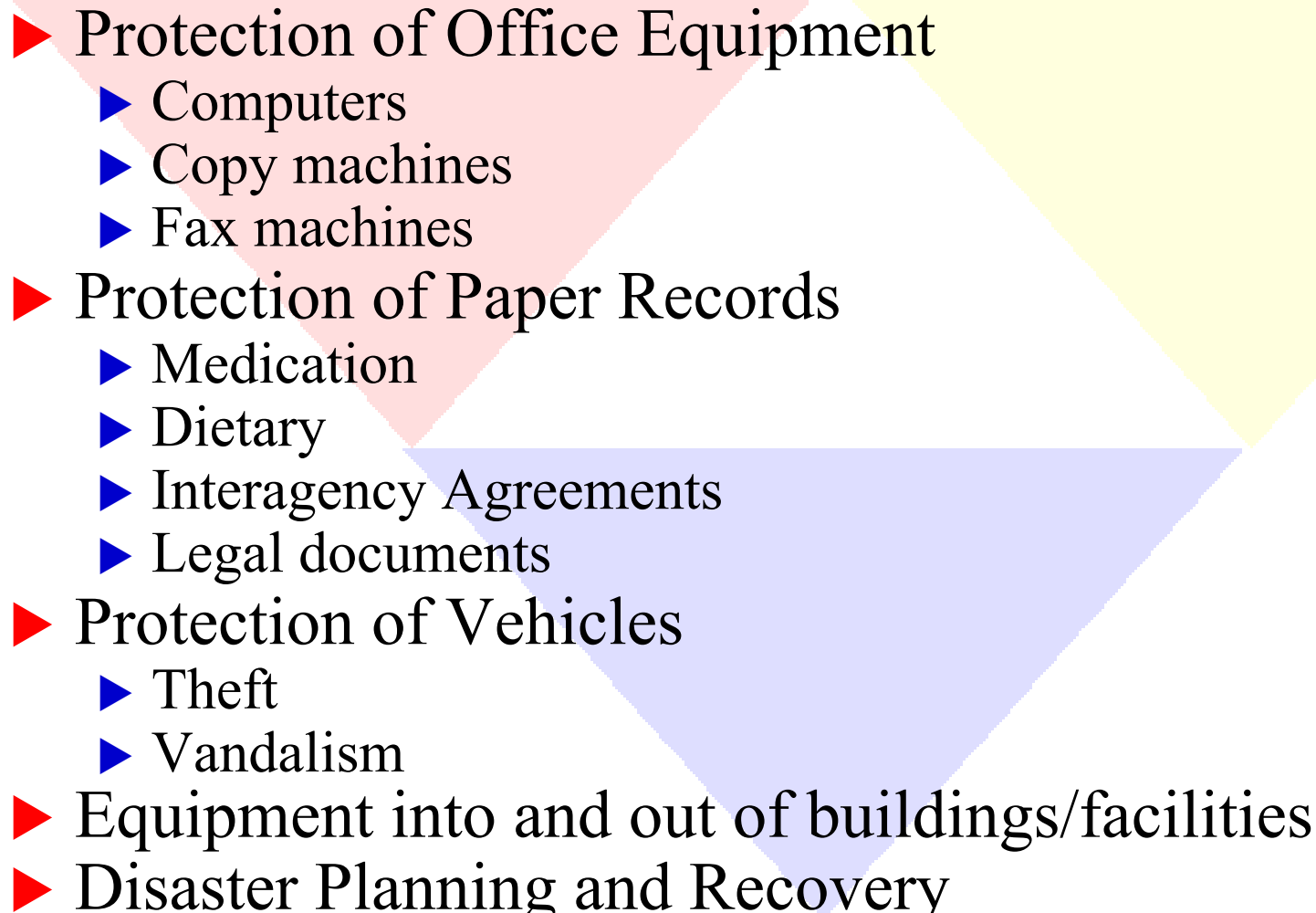
Security Drivers

- 
- ▶ Clients
 - ▶ Facility/forensic residents
 - ▶ ISL and Residential Care
 - ▶ Staff
 - ▶ September 11, 2001
 - ▶ CIMOR
 - ▶ HIPAA
 - ▶ Privacy
 - ▶ Security

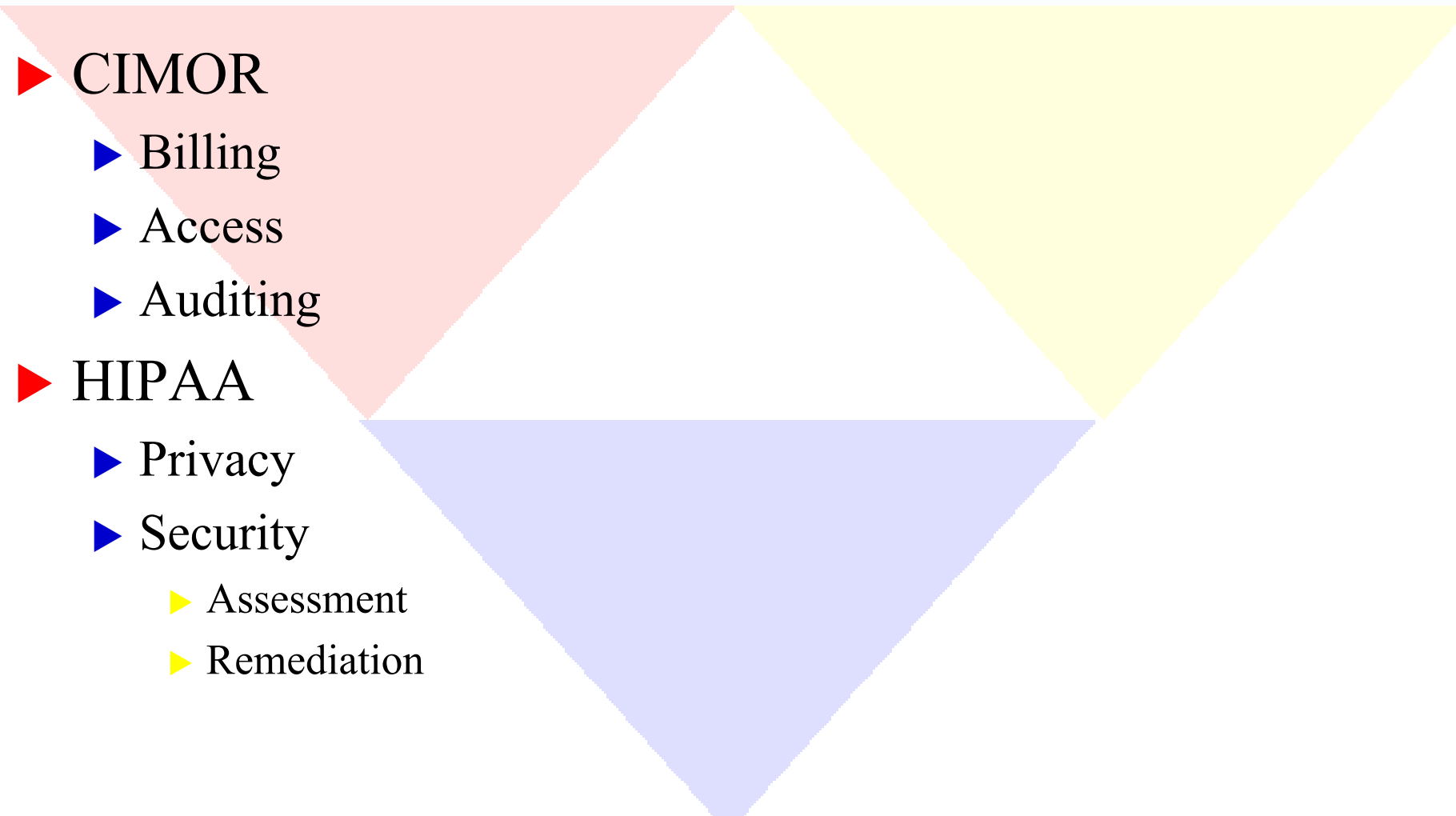
Security is More Than an IT Issue

- 
- ▶ Safety of clients/staff/visitors
 - ▶ Identification of staff/visitors
 - ▶ Evacuation plans
 - ▶ Admittance to and exiting buildings/facilities
 - ▶ Keys and key pads
 - ▶ Swipe cards
 - ▶ Nothing
 - ▶ Reception and hosting of visitors
 - ▶ Who, Why, Where, For how long
 - ▶ Mail

Security is More Than an IT Issue

- 
- ▶ Protection of Office Equipment
 - ▶ Computers
 - ▶ Copy machines
 - ▶ Fax machines
 - ▶ Protection of Paper Records
 - ▶ Medication
 - ▶ Dietary
 - ▶ Interagency Agreements
 - ▶ Legal documents
 - ▶ Protection of Vehicles
 - ▶ Theft
 - ▶ Vandalism
 - ▶ Equipment into and out of buildings/facilities
 - ▶ Disaster Planning and Recovery

IT Security Issues

- 
- ▶ CIMOR
 - ▶ Billing
 - ▶ Access
 - ▶ Auditing

- ▶ HIPAA
 - ▶ Privacy
 - ▶ Security
 - ▶ Assessment
 - ▶ Remediation

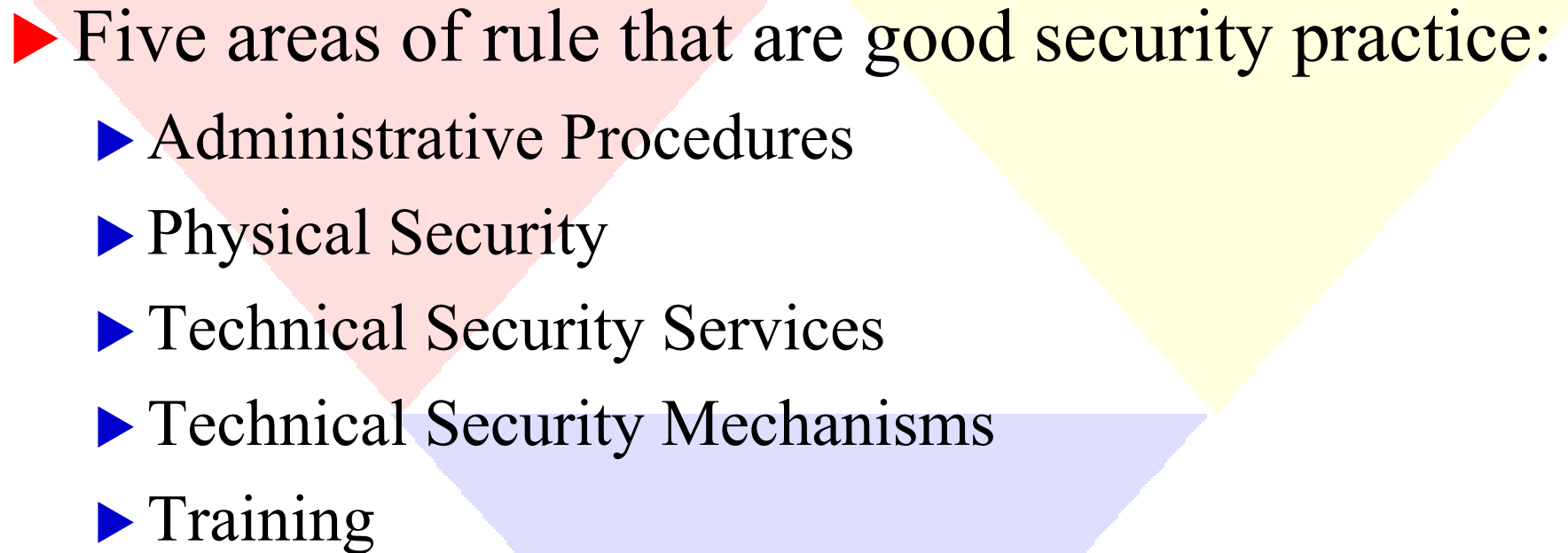
Status of Final HIPAA Security Regulation

- ▶ NPRM published August 12, 1998
- ▶ No guidance from DHHS on when final rule to be published – in “clearance process”
- ▶ CMS has publicly stated that the electronic signature components have been removed from final rule

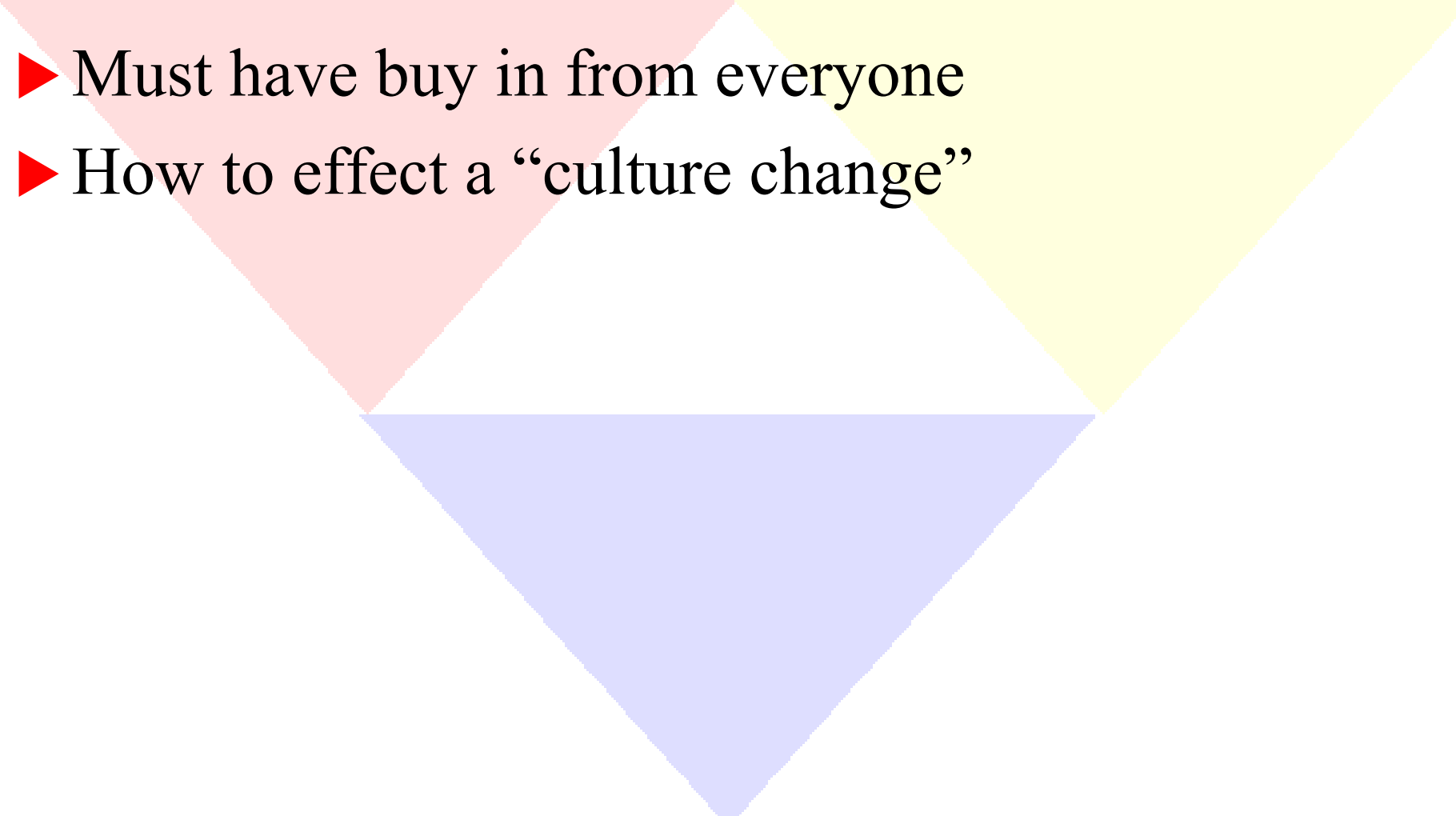
Why DMH Proceeded with Security Assessment Process

- ▶ Non-IT security issues
- ▶ CIMOR
 - ▶ Resolves only technical issues
- ▶ Overlap with HIPAA Privacy Regulation
 - ▶ CFR 45 §164.530(c)
- ▶ All indications are that the Security Rule would not change substantially from the NPRM.

Why DMH Proceeded with Security Assessment Process

- 
- ▶ Five areas of rule that are good security practice:
 - ▶ Administrative Procedures
 - ▶ Physical Security
 - ▶ Technical Security Services
 - ▶ Technical Security Mechanisms
 - ▶ Training

The Challenges

- 
- ▶ Must have buy in from everyone
 - ▶ How to effect a “culture change”

The DMH HIPAA Security Assessment Process

- ▶ Security Workgroup formed in March 2001
- ▶ Developed draft Security Officer job description
- ▶ Recommended security assessment tool – based on SNIP
- ▶ Developed List of Deliverables
- ▶ All facilities appointed Security Officers

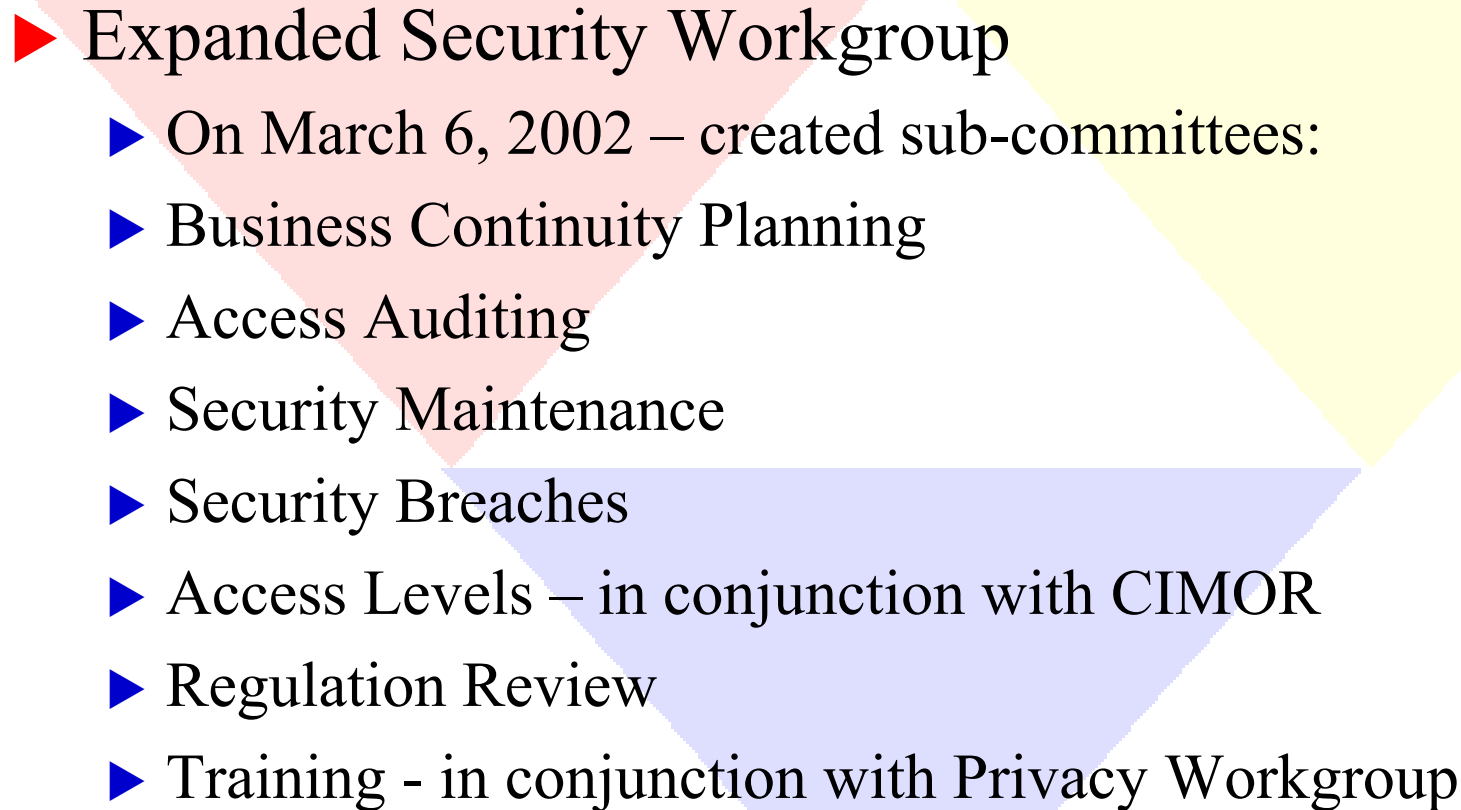
The DMH HIPAA Security Assessment Process - Continued

- ▶ Appointed Central Office Interim Security Officer
- ▶ OIS developed online entry application
- ▶ Mandatory facility security officer training held December 20, 2001

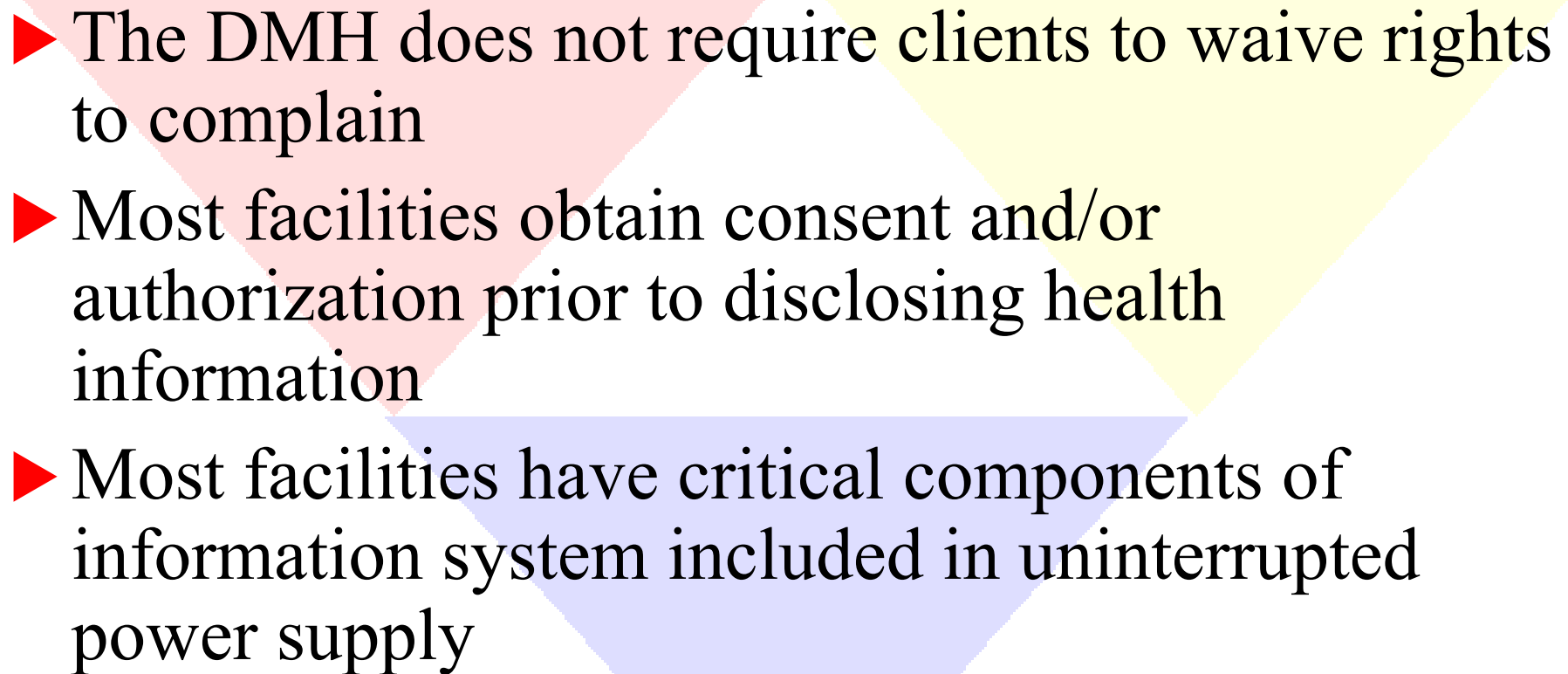
The DMH HIPAA Security Assessment Process - Continued

- ▶ Pilots began security assessment process January 2, 2002
 - ▶ CMRC
 - ▶ Nevada Hab Center
 - ▶ Western MO MHC
- ▶ Statewide security assessments began January 23, 2002
- ▶ Completed March 15, 2002
- ▶ Appointed Ed Meyers as DMH Security Officer

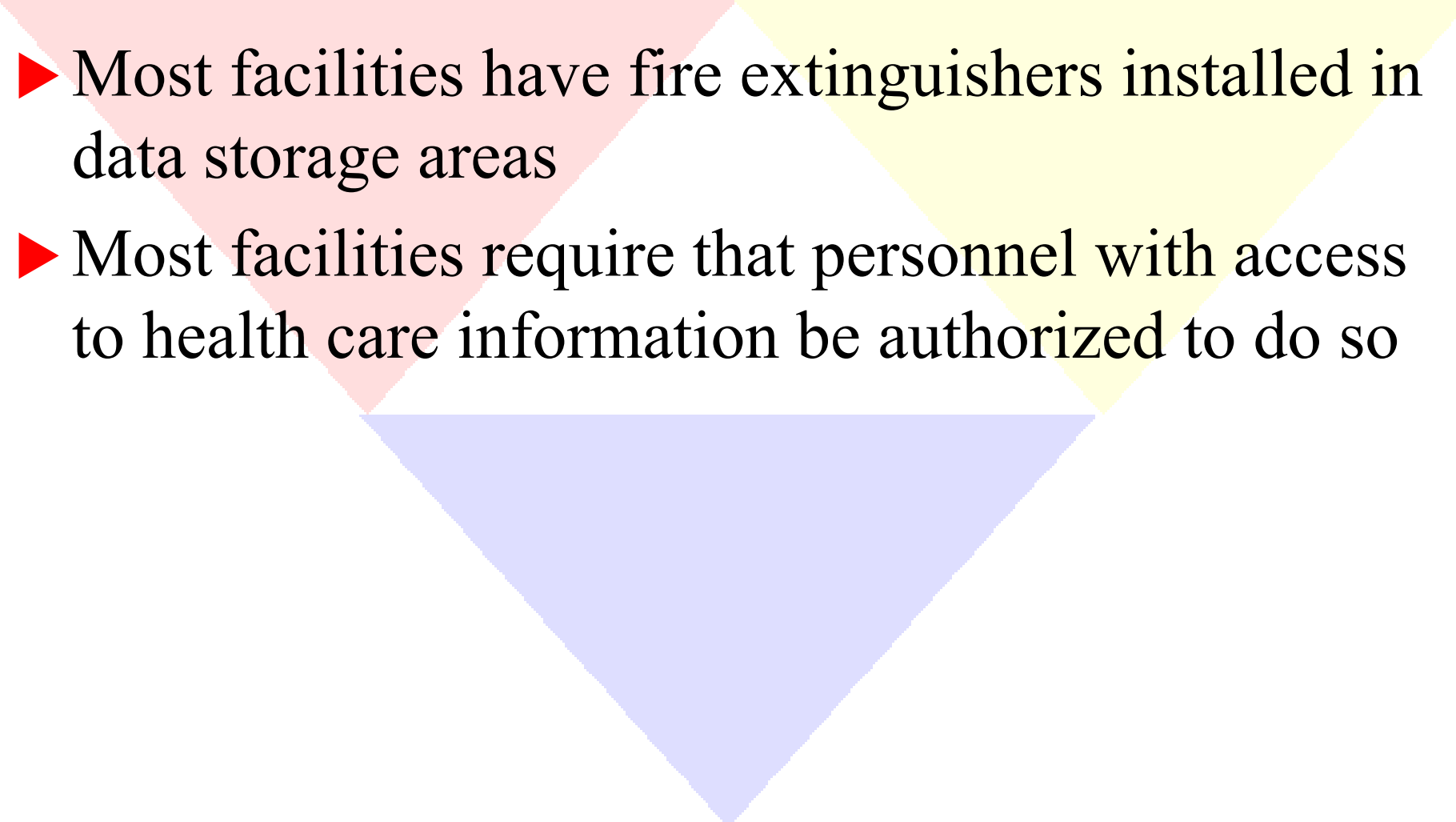
The DMH HIPAA Security Assessment Process - Continued

- 
- ▶ Expanded Security Workgroup
 - ▶ On March 6, 2002 – created sub-committees:
 - ▶ Business Continuity Planning
 - ▶ Access Auditing
 - ▶ Security Maintenance
 - ▶ Security Breaches
 - ▶ Access Levels – in conjunction with CIMOR
 - ▶ Regulation Review
 - ▶ Training - in conjunction with Privacy Workgroup

What the Assessment Shows

- 
- ▶ The DMH does not require clients to waive rights to complain
 - ▶ Most facilities obtain consent and/or authorization prior to disclosing health information
 - ▶ Most facilities have critical components of information system included in uninterrupted power supply

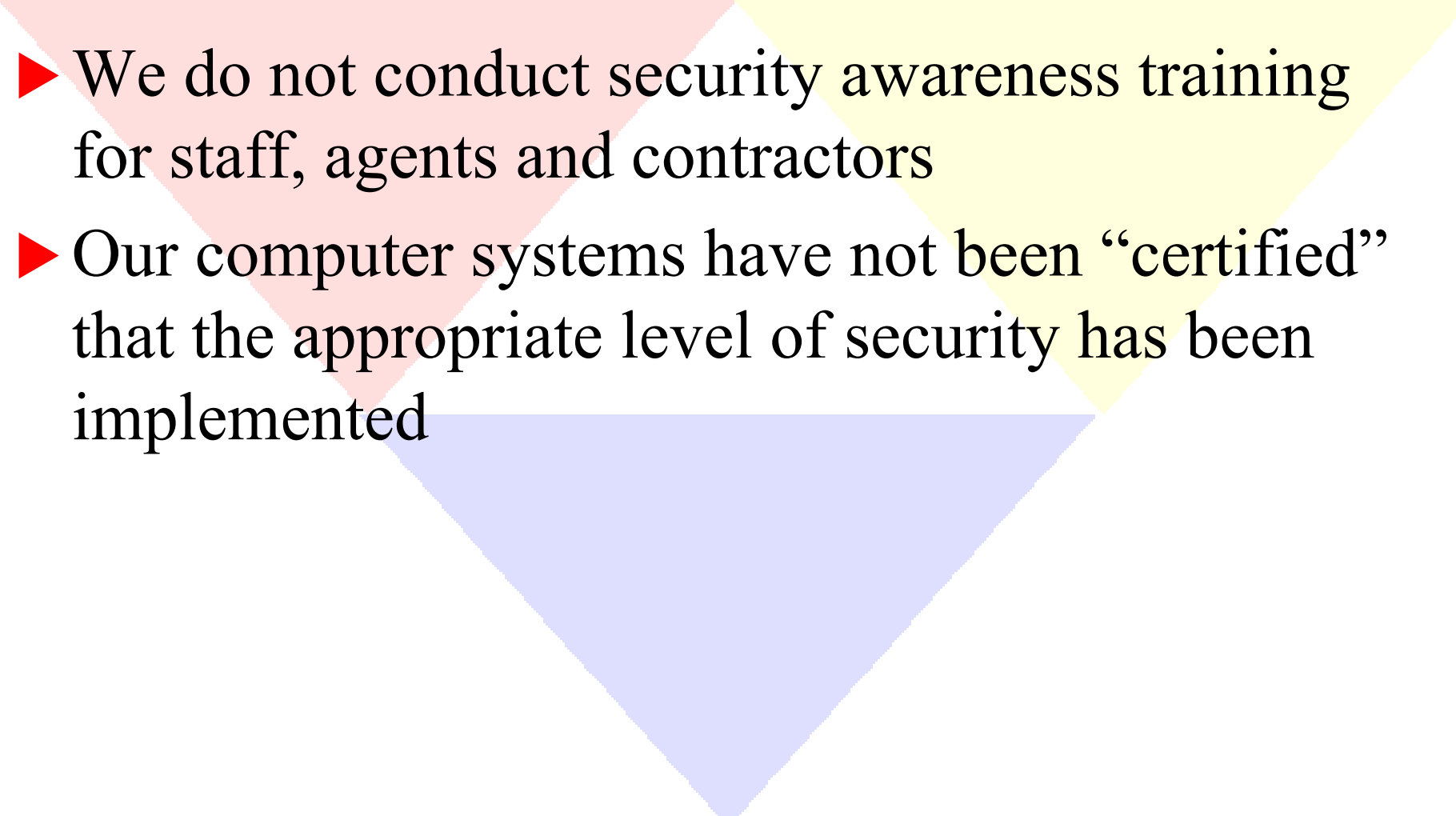
What the Assessment Shows

- 
- ▶ Most facilities have fire extinguishers installed in data storage areas
 - ▶ Most facilities require that personnel with access to health care information be authorized to do so

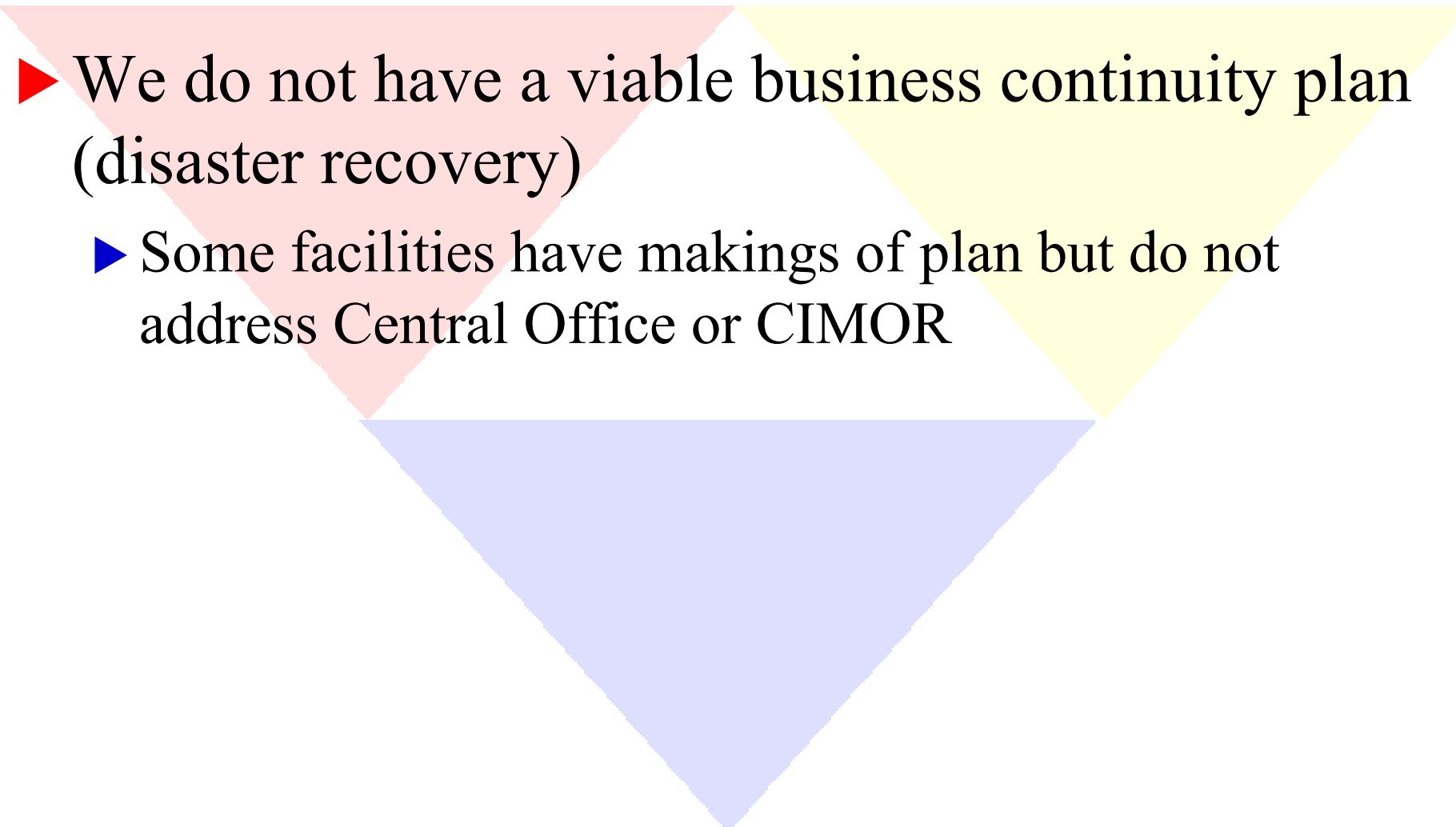
What the Assessment Shows

- ▶ We restrict testing and revision of our systems to only authorized personnel
- ▶ We have some policies regarding workstation use
 - DOR 1.915
- ▶ We do have unique user ID's and passwords

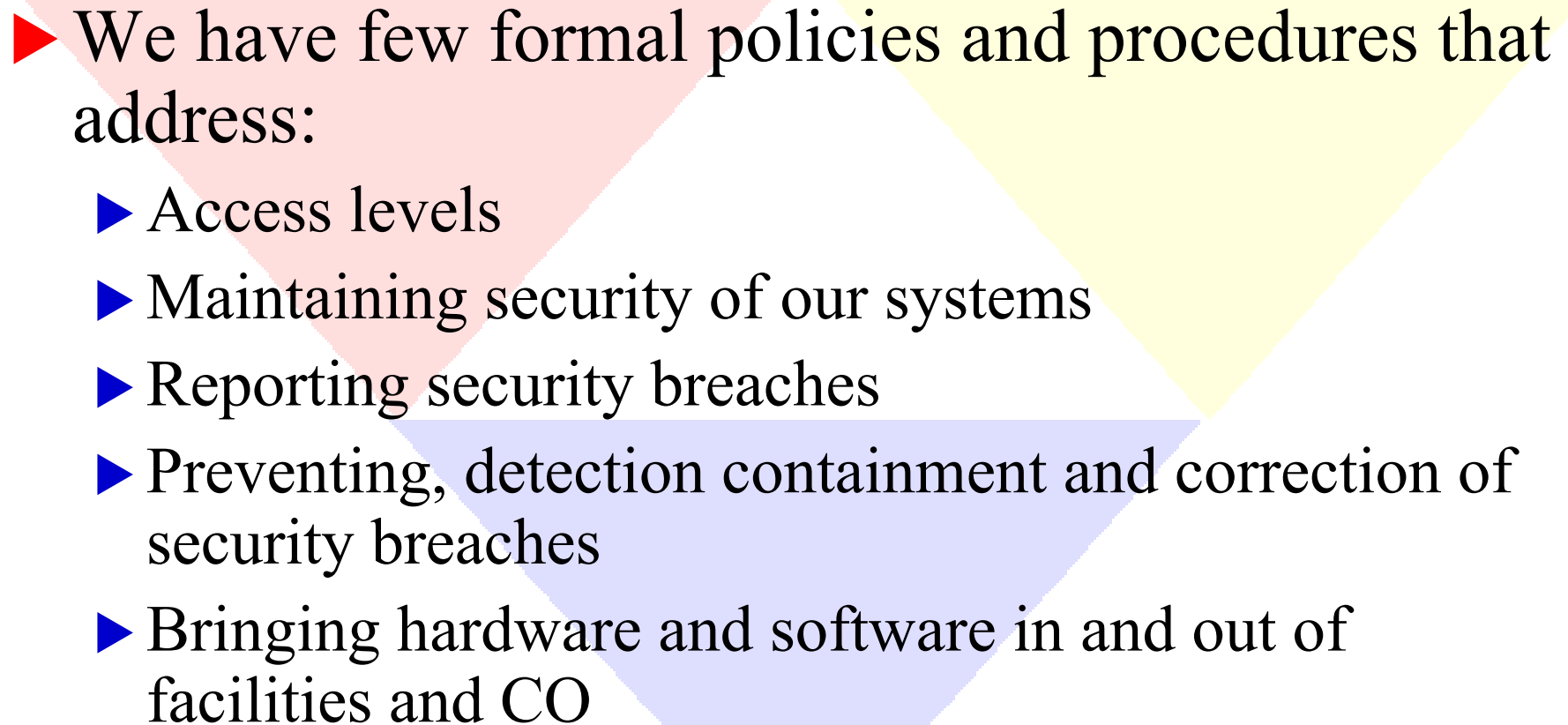
What the Assessment Shows

- 
- ▶ We do not conduct security awareness training for staff, agents and contractors
 - ▶ Our computer systems have not been “certified” that the appropriate level of security has been implemented

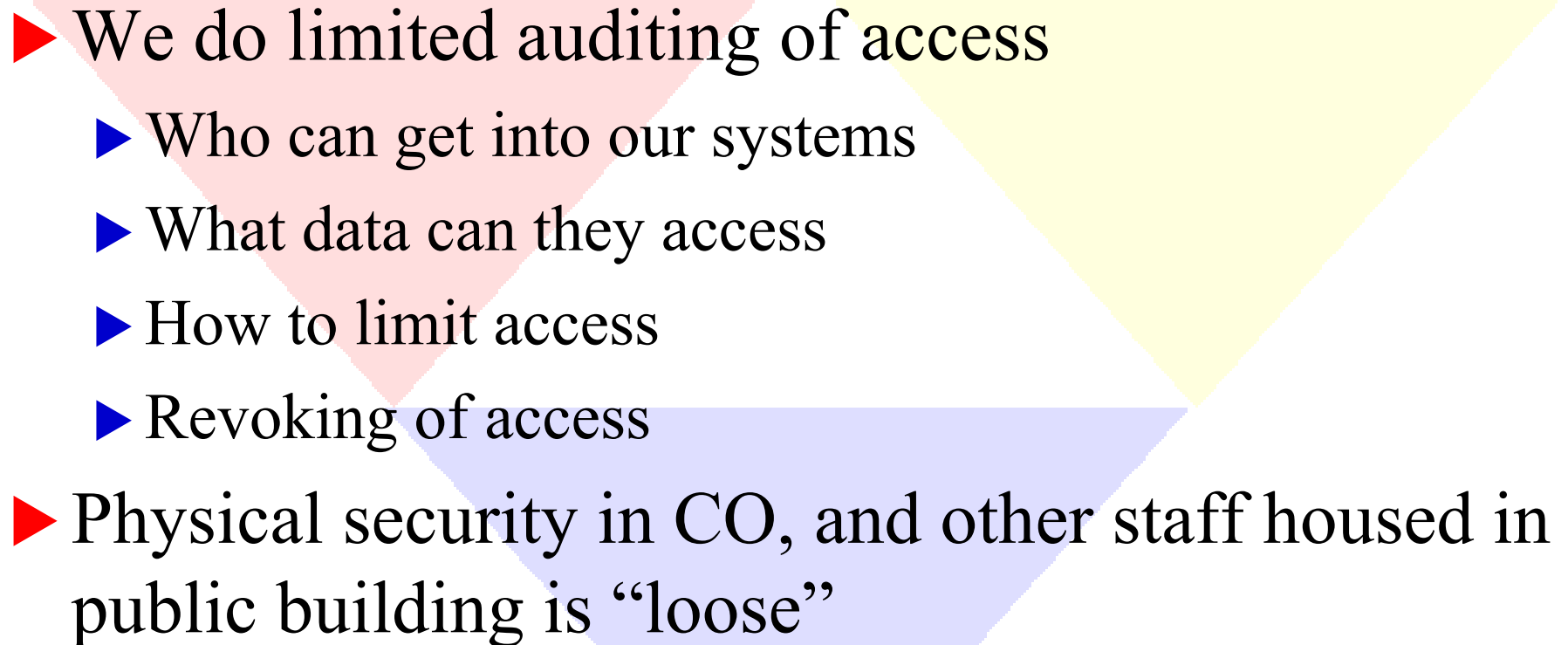
What the Assessment Shows

- 
- ▶ We do not have a viable business continuity plan (disaster recovery)
 - ▶ Some facilities have makings of plan but do not address Central Office or CIMOR

What the Assessment Shows

- 
- ▶ We have few formal policies and procedures that address:
 - ▶ Access levels
 - ▶ Maintaining security of our systems
 - ▶ Reporting security breaches
 - ▶ Preventing, detection containment and correction of security breaches
 - ▶ Bringing hardware and software in and out of facilities and CO

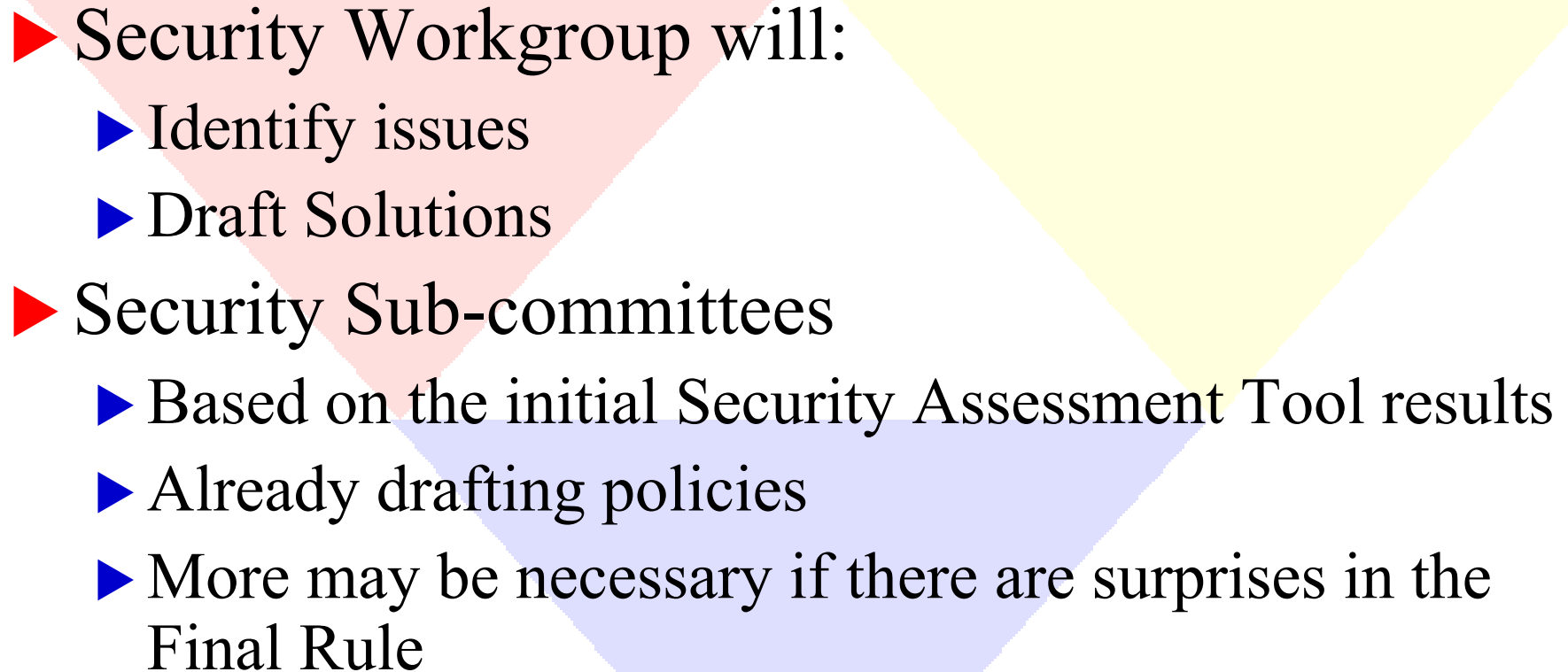
What the Assessment Shows

- 
- ▶ We do limited auditing of access
 - ▶ Who can get into our systems
 - ▶ What data can they access
 - ▶ How to limit access
 - ▶ Revoking of access
 - ▶ Physical security in CO, and other staff housed in public building is “loose”

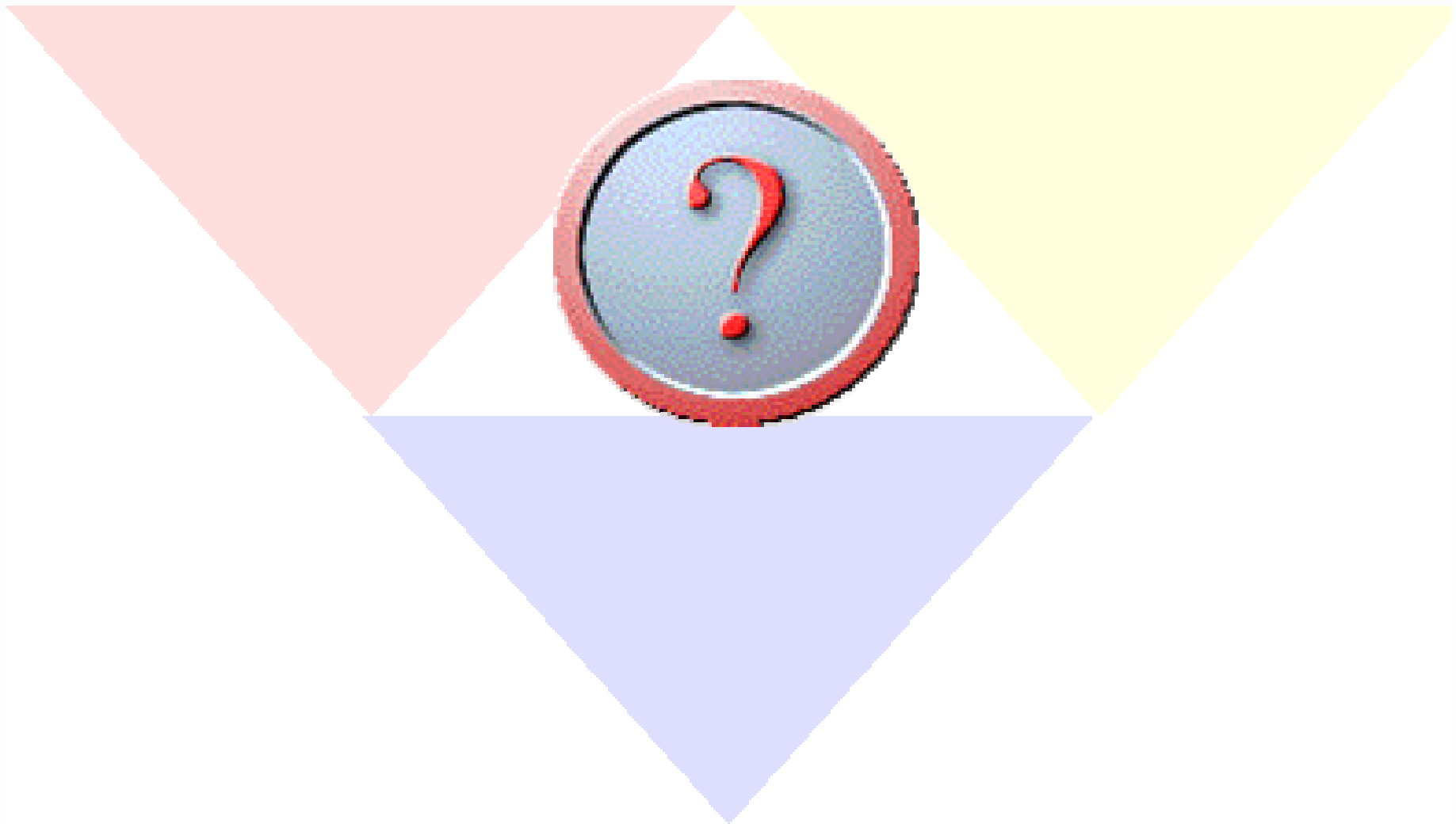
Where Do We Go From Here?

- ▶ Hope that the Security Rule is published soon, however:
 - ▶ Privacy Rule states “A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information”
 - ▶ Required by April 14, 2003.
 - ▶ Training to begin in October 2002
 - ▶ CIMOR

Where Do We Go From Here?

- 
- ▶ Security Workgroup will:
 - ▶ Identify issues
 - ▶ Draft Solutions
 - ▶ Security Sub-committees
 - ▶ Based on the initial Security Assessment Tool results
 - ▶ Already drafting policies
 - ▶ More may be necessary if there are surprises in the Final Rule

Questions?



Helpful Websites

- ▶ DHHS Web Page (Select HIPAA under topics)
<http://www.hhs.gov/>
- ▶ DHHS Office of Civil Rights Privacy Regulation
<http://www.hhs.gov/ocr/hipaa/>
- ▶ American Health Information Management Association
<http://www.ahima.org>
- ▶ National Workgroup for Electronic Data Interchange
<http://www.snip.wedi.org>
- ▶ HIPAAlive List Serve Group
<http://www.hipaadvisory.com/live/>
- ▶ Department of Mental Health HIPAA Page
<http://www.modmh.state.mo.us/homeinfo/hipaa/>

Questions & Discussion



The End